SailPoint

Report

The Horizons of Identity Security

Harnessing the power of identity security to bend the cybersecurity value curve

2024-2025

Executive summary

Organizations across sectors around the world face a dual challenge: they must counter increasingly sophisticated and pervasive cyber threats while grappling with constrained budgets and relentless cost-cutting.

The pressures are especially intense in identity security where attack surfaces grow and IT budgets tighten as organizations scale, yet internal and external stakeholders increasingly demand better security and digital experiences. Employees need quick and easy access to business applications, for example, and customers demand seamless omnichannel interactions; both are less tolerant of usernames and passwords.

Getting identity right is difficult, but it is critical in reducing risk and improving customer experience. The addition of every new customer, employee, contractor, and machine identity presents risks - along with opportunities to create business value. Unlike other cyber capabilities, identity security has the power to secure an organization while transforming the way customers interact with the business. This can lead to real revenue impact, build the trust of customers, employees, and other stakeholders, and yield lasting competitive advantages.

To lobby their organizations for the necessary financial and human resources, IT leaders need to understand and explain what will drive the most value—and use those resources wisely. When it comes to identity security, the case for investment is strong.

Our research and experience suggest that every dollar invested in identity security delivers disproportionately higher returns, "bending" the identity security-to-value curve. These disproportionately higher returns are observed through higher risk reduction, business value, and productivity. Strategic investment in IAM delivers outsized returns by unlocking new value pools such as enhanced capability coverage and data analytics, automation, lower cyber insurance premiums, and improved compliance.

A leading tech retailer, for example, reduced cyber risk by more than two-thirds by setting appropriate privileges for about 6,000 accounts and automating identity security and governance. A major financial institution reduced costs and improved outcomes by implementing an AI-based risk management tool, saving $300 per identity onboarded. A prominent bank improved productivity by automating manual IAM tasks, including 90% of all access requests.

Over the last three years, SailPoint has surveyed identity and access management (IAM) decision-makers across the globe to assess their capabilities across identity security horizons and define the future of identity. The 350 decision-makers we surveyed in July 2024 included senior leaders in information technology, cybersecurity, and risk; more than half work for organizations with more than 10,000 employees, and more than half work in the finance or technology sectors. (For details on survey demographics, please 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

What we found

Based on our survey of identity security decision-makers and interviews, the following insights and themes emerged:

- **Most organizations have significant opportunities to realize the full potential of identity security.** Of the organizations we surveyed, 41% remain in Horizon 1. 23% are in Horizon 2, 26% in Horizon 3, and ~10% in Horizons 4 and 5. From 2023 to 2024, only 3% moved beyond Horizon 1, and only 1% from Horizon 3 to 4, suggesting that the full value of identity security remains untapped for the majority of organizations.
- **Identity security is core to overall enterprise security.** Horizon 3 and 4+ organizations have better overall security posture. For example, they have 50% higher NIST CMMI scores, as compared to Horizon 1 and 2 organizations, suggesting investment in identity is an essential step toward securing organizations at large.
- **Organizations that advance to higher identity security horizons can "bend the curve"—delivering disproportionate economic impact.** More mature organizations gain disproportionate reductions in risk, higher topline business value, and increased workforce productivity.

- **Organizations at Horizon 3 and beyond reduce risk through higher identity coverage.** The gap in coverage is especially wide for third-party and machine identities, where the survey showed Horizons 3 and 4 organizations have 20-50% higher coverage of third-party and machine identities.
- **Machine identities are growing faster than all other identity types,** making coverage of these identities increasingly important for organizations of all maturity levels. Growth is fueled by the increasing use of cloud workloads and AI applications such as copilots, prompts, ML models, and bots that tend to be highly fragmented within organizations and necessitate non-human account access. Organizations at or beyond Horizon 3 are better equipped to secure them, given their higher coverage.
- **Mature identity security organizations are twice as likely to use identity data to create actionable security or business intelligence.** They use data to enable new use cases, for example, such as intelligent guidance for user access, context-aware security policies, and intelligent access reviews.
- **AI-powered use case adoption is relatively low across organizations,** though Horizons 1-2 still trail Horizons 3 and 4. About half of those at Horizon 4 have adopted top AI-powered use cases, including role-access reconciliation, adaptive authentication, and privileged access.
- **Organizations with mature identity security have the foundations to invest in scalable GenAI-powered use cases**. Many Horizon 4 organizations are now developing GenAI capabilities to enhance engineering and expand identity security, whereas Horizon 1-2 organizations tend to prioritize automation of repetitive helpdesk tasks through more mainstream solutions, such as AI chat bots.
- **Horizon 3 and 4 organizations scale identity coverage and capabilities without growing their IAM workforces** by improving efficiency with advanced IAM solutions and shifting from helpdesk to engineering-led support models.
- **Horizon 3 and 4 organizations have 15-50% higher adoption of privileged access governance capabilities.** By investing in solutions beyond credential vaulting and session management, they simplify access approval and requests while enhancing threat analytics for privileged accounts.
- **Identity security is a key to mitigating increases in insurance premiums.** Insurers have improved their risk assessment strategies, while raising premiums to more accurately reflect higher risk profiles. They now assess the security capabilities of nearly every organization before setting premiums. Demonstrating advanced identity security maturity helps reduce cyber insurance premiums.
- **Identity-related regulations have grown sevenfold since 2010** globally across regions and industries. As a result, organizations must invest in maturing identity security capabilities to navigate complex regulatory landscapes and ensure compliance.

The value of identity security will continue to rise as cyber threats multiply; legislators, regulators, investors, and insurers raise their security expectations; and customers, employees, and business partners increasingly seek trusted and seamless digital experiences.

Advancing identity security requires focused resources - time, money, talent, and the attention of senior leaders - and the costs of inaction can be far higher. Gaps in identity security can slow digital transformations and cloud migrations, complicate mergers and divestitures, stifle innovation, and attract bad actors. One negative identity experience can mean losing a customer forever; a major breach can have catastrophic financial and reputational consequences.

Advancing identity security requires focused resources - time, money, talent, and the attention of senior leaders - the costs of inaction can be far higher.

The good news is that organizations that harness the power of identity can overcome these challenges and deliver disproportionately higher returns. A unified approach to identity - encompassing data, operations, and users - can reduce risk, enhance business value, and drive substantial improvements in business productivity.

Identity drives disproportionately higher returns and enables organizations to build trust with customers, employees, and partners, expanding total economic benefits and competitive advantages.

Chapter 1:

Advances in technology will shape the future of identity security

In the last few years, our experience and research have confirmed that the future of identity security will be shaped by integrated identity programs. The pillars of next-generation identity security include:

- **Integration across diverse technology environments:** Unified access controls provide visibility across all identity types, integrate with security operations, and support machine identity management and actionable intelligence.
- **Dynamic trust models:** Zero-trust architecture and AI-driven access models enable dynamic authorization, adjusting permissions based on behavior and context-aware policies.
- **Federated identities:** Federated access allows organizations to manage diverse identities across digital environments, enhancing security and user experience, with early adoption of decentralized protocols and digital wallets.
- **Frictionless access:** Automated privileged access and password-less authentication using passkeys, biometrics, and certificates ensure seamless and secure user authentication.

Over the past year, three trends have emerged that complement these pillars of the future of identity:

- **Machine identity management:** With the rise of AI and automated bots, organizations need to manage more non-human accounts, such as those used by copilots and machine learning models.
- **Integrated identity data layer:** An integrated data layer is key to generating actionable intelligence and insights, exemplified by the development of context-rich identity graphs to create unified employee and customer profiles.
- **Context-aware policy enforcement**: Access decisions are increasingly driven by AI-powered analytics, which use context-aware policies to enhance security through anomaly detection, identity pattern recognition, and behavior analysis.

Organizations can use these forward-thinking capabilities to set the north star vision for their identity security strategy, which can guide innovative initiatives and capabilities that improve identity security outcomes and create value for customers, employees, shareholders, and other stakeholders.

Exhibit 1:
The future of identity will be defined by 4 key elements

Evolving regulatory and risk landscape continues to shape these four elements

Identity security fabric will become the nerve center of future security operations – IT workloads are complex and transcend network, infra, and geographic perimeters while cyber attacks have become even more sophisticated in exploiting any fault points in security posture. In that context, identity security fabric will protect beyond network perimeter, identifying the blast radius of any incident, detecting the compromise, and responding fast to contain and recover.

Proliferation of identity security related regulations and industry standards across the globe and across industries is expected to drive increased expectations on identity security controls and compliance.

Note: Accelerated adoption of AI 'copilots' and decision-support models may enhance security, user experience, and developer efficiency for building and maintaining scalable identity security platforms, while introducing risks, such as the potential for AI-driven identity compromise.

Exhibit 2:

Proof points in the last 12 months support progress across the 4 elements shaping the future of identity

Integrated identity program

The U.S. cybersecurity strategy implementation plan was updated in March 2024, enhancing interagency collaboration through 100 initiatives aimed at advancing strategic objectives, including investments in digital identity innovations and standards to bolster security and privacy[1]

2024's inaugural U.S. Cybersecurity Posture Report highlights enhanced identity access management aspirations via strategic federal initiatives[2]

OCSF, an open-source extensible framework for developing schemas, was updated to include remediation events, new event classes, and threat intelligence profiles[3]

Dynamic trust models

In February 2024, the Cybersecurity and Infrastructure Security Agency established the Zero Trust Initiative Office to help federal agencies adopt zero-trust security and provide training, guidance, and tools to improve compliance with the federal zero-trust strategy by year-end[4]

Veriff Fraud Index 2024 report found a 20% rise in fraud year-over-year with 86% of surveyed consumers demanding more robust fraud prevention capabilities, pointing to the need for enhanced identity management, including through dynamic trust[5]

Federated identities

The Identity & Access Forum launched the industry's first mobile driver's license (mDL) use case template to facilitate widespread adoption by relying parties such as law enforcement and retailers[6]

Council of EU adopts revised European Digital Identity (eID) regulation, requiring all EU citizens to have access to a secure digital wallet by 2026[7]

Australia allocates $288 million to implement the Digital ID Bill, set for enactment in November 2024, establishing a Digital ID system with a voluntary Accreditation Scheme to enhance security, streamline interactions, and reduce identity theft[8]

Frictionless access

Adobe, Apple, Google and other brands have facilitated password-less sign-ins for over 13 billion accounts; In 2024 FIDO report, 62% of surveyed consumers are aware of passkeys, 53% have enabled them on at least one account, and 23% use them regularly, citing a 61% boost in security and 58% in convenience compared to traditional passwords[9]

Major airlines such as Delta and Lufthansa have adopted biometric boarding processes to enhance security and improve passenger experience, using facial recognition to check in, drop off bags, pass through security, and board flights without a physical ID[10]

Evolving regulatory and risk landscape continues to shape these four elements

AI Act adopted by the Council of EU, establishing the first legal framework on AI to address risks, ensures trustworthy AI, and supports businesses, with implementation phased over the following years[11]

By the end of 2024, India will implement the Digital Personal Data Protection Act, introducing strict compliance measures and establishing the Data Protection Board to investigate breaches and impose monetary penalties for violations[12]

NIST updated its Cybersecurity Framework (CSF) to include the "Govern" pillar, bolstering its focus on enterprise risk management (e.g., integrating cybersecurity risks into broader organizational processes and comprehensive risk monitoring)[13]

SEC's new cybersecurity disclosure rules mandate immediate disclosure of material cybersecurity incidents within 4 business days and annual reporting on risk management, strategy, and governance[14]; CISA also instituted an incident reporting mandate[15]

[1] https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

[2] https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report- on-the-Cybersecurity-Posture-of-the-United-States.pdf

[3] https://aws.amazon.com/blogs/opensource/from-data-chaos-to-cohesion-how-ocsf-is-optimizing-cyber-threat-detection/

[4] https://fedscoop.com/cisa-zero-trust-initiative-office-sean-connelly/

[5] https://www.veriff.com/fraud/news/veriff-fraud-industry-pulse-survey-key- findings

[6] https://www.securetechalliance.org/identity-access-forum-launches- industrys-first-template-for-building-mobile-drivers-license-use-cases/

[7] https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/ european-digital-identity-eid-council-adopts-legal-framework-on-a- secure-and-trustworthy-digital-wallet-for-all-europeans/

[8] https://www.forbes.com/sites/benjaminlaker/2024/05/25/what-leaders- need-to-know-about-the-australian-digital-id-bill-2024/

[9] https://www.theregister.com/2024/05/02/microsoft_google_passkeys/

[10] https://news.delta.com/delta-expands-digital-id-program-lax-lga-and-jfk- touchless-airport-experience

[11] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

[12] https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and- cybersecurity-law/20230818-india-passes-long-awaited-privacy-law

[13] https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[14] https://www.reuters.com/legal/legalindustry/secs-new-cybersecurity-disclosure-rules-decoded-what-they-mean-investors-2024-05-31/

[15] https://www.mayerbrown.com/en/insights/publications/2024/03/proposed-rule-issued-to-implement-cyber-incident-reporting-for-critical-infrastructure-act

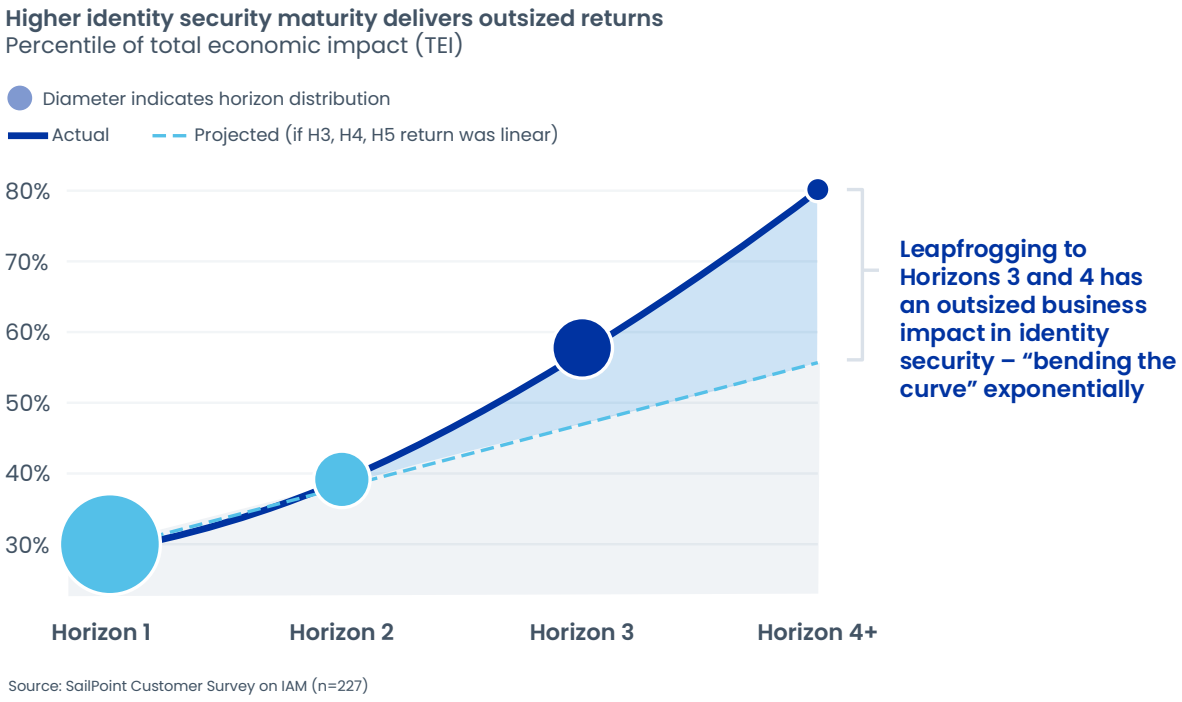
Chapter 2:

Investments in identity security can “bend the curve”

Our 2024 survey of identity security decision-makers shows that organizations that invest to reach mature identity security get disproportionately higher returns. Spending on cybersecurity, like many other investments, typically delivers linear returns. However, the IAM maturity-to-value curve grows exponentially, as shown in the exhibit [below], meaning organizations in Horizons 3 and 4 reap compounding benefits from increasingly mature identity ecosystems.

This should drive a major shift in the way organizations think about investing in cybersecurity capabilities—and suggests that investments in IAM may deliver more value than investments in other cyber capabilities.

Exhibit 3:
Organizations with mature identity security deliver disproportionately higher returns for every dollar spent

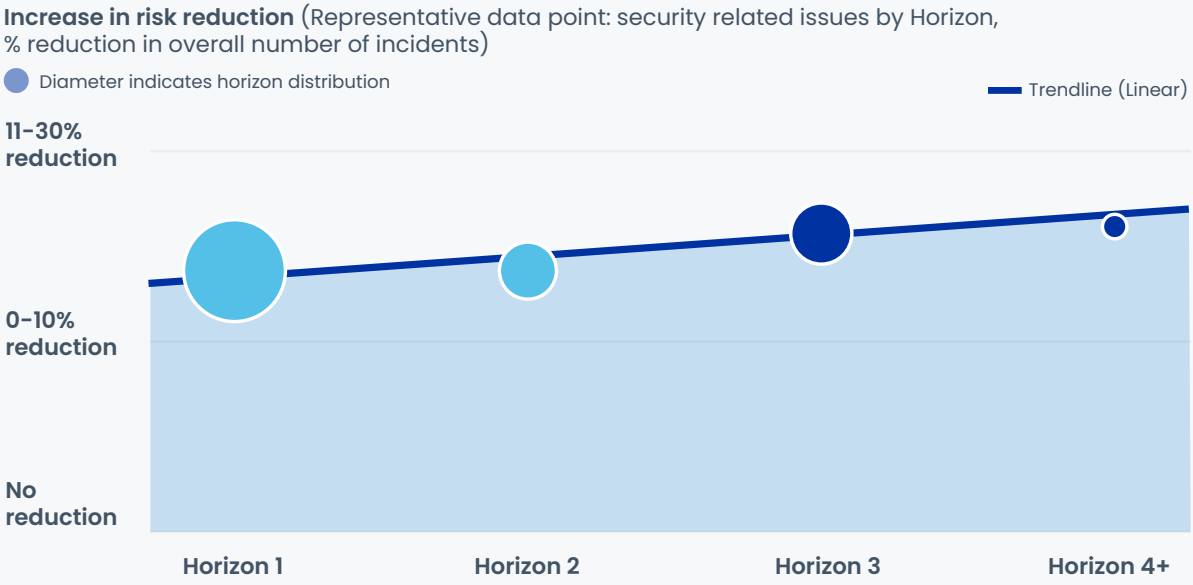


Source: SailPoint Customer Survey on IAM (n=227)

In the exhibit [above], value is plotted against maturity, where maturity is measured across the Horizons of identity security. We measure return, or value, as a function of Total Economic Impact (TEI), calculating it based on how an organization scores in three dimensions—risk reduction, business value, and workforce productivity—as it moves across horizons.

For example, Horizon 4 organizations have lower risk as measured by fewer identity-related security issues, generate more business value through accelerated digital transformations, and increase productivity by automating IAM. We normalize these discrete findings across risk, business value, and workforce productivity and then compile them into an aggregate TEI score. In this section, we detail our findings for the three dimensions where organizations see disproportionately higher returns with increased maturity.

Exhibit 4:
Risk reduction: Moving through identity security horizons reduces the attack surface for potential breaches



Source: SailPoint Customer Survey on IAM (n=227): Question 5.02 "Have you noticed a decrease in identity related security issues stemming from your investment in IAM solutions over the past year?

Organizations disproportionately reduce risk as they progress through horizons. In the exhibit [above], risk reduction is plotted against maturity, where higher Horizon organizations see larger reductions in risk. According to the survey results, 63% of organizations that invest to reach mature identity security see on average more than 10% (and up to 30%) reduction in identity-related security issues, while lower-maturity organizations severely lag behind.

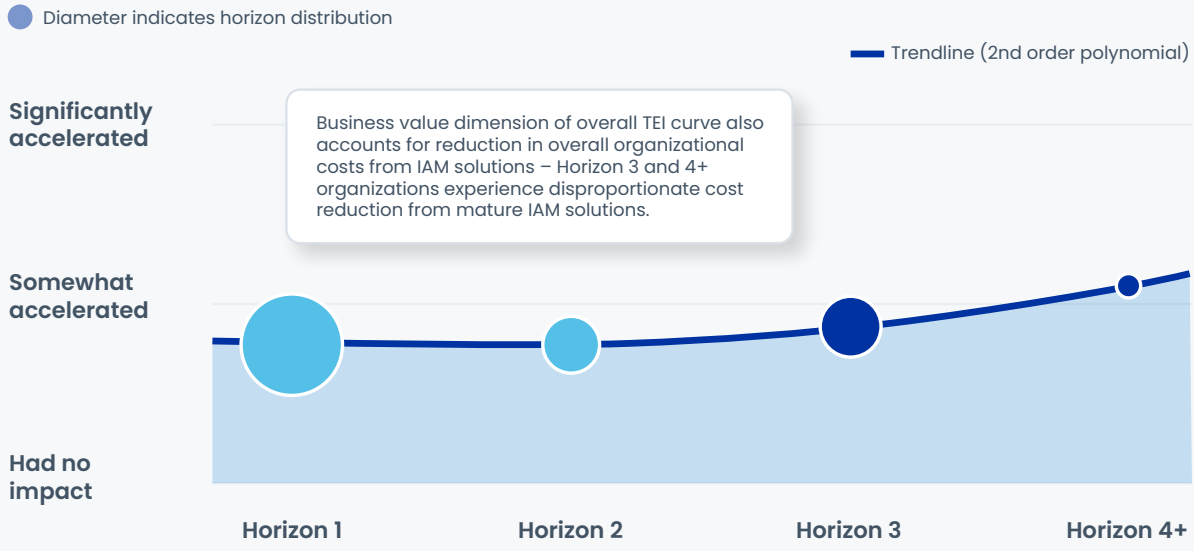
While it is no surprise that investments in capabilities reduce identity-related security issues, the reductions are significantly higher for Horizon 3 and 4 organizations. These organizations are better equipped to shrink attack surfaces and minimize the blast radius of incidents.

Organizations with advanced identity security capabilities can drive topline revenue impact by accelerating product time to market. In our survey, IT leaders were asked to what extent the implementation of identity management solutions accelerated digital transformation within their organizations. The exhibit [below] plots their responses against maturity, where Horizon 3 and 4 responses for digital transformation acceleration are on average 16% higher than Horizon 1 responses. We found that advanced identity security accelerates digital transformations, enabling faster development cycles and speed to market, increasing revenue. Horizon 3 and 4 organizations do this while providing the same level of security and reducing friction for users, as shown in the exhibit [below].

Exhibit 5:

Business value: Organizations with advanced identity capabilities experience faster time to market and reduced friction

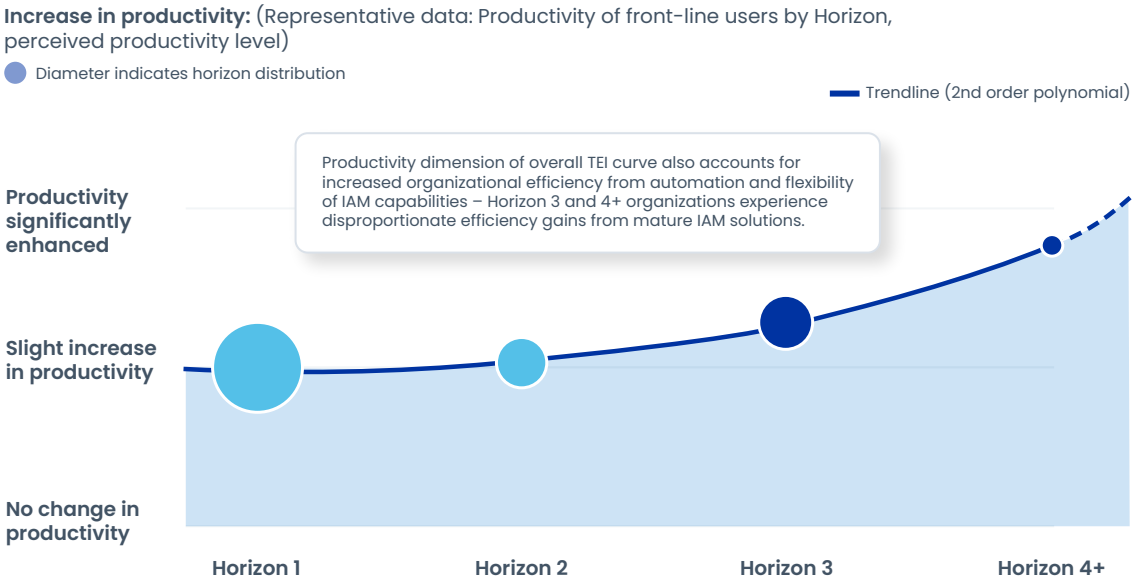
Increase in business value: (Representative data: Impact of IAM solutions on speed of digital transformation by Horizon, perceived transformation acceleration)



Source: SailPoint Customer Survey on IAM (n=227): Question 7.18 "To what extent has the implementation of identity management solutions accelerated digital transformation initiatives in your organization?"

Organizations that reach mature identity security experience significantly higher productivity gains from IAM automation use cases. In our survey, IT leaders were asked how the implementation of IAM automation use cases affected the productivity of their front-line users. The exhibit [below] plots their responses against maturity, where Horizon 4 responses for productivity gains were 22% higher than Horizon 1 responses. Front-line users in Horizon 3 and 4 organizations get faster access when joining the company or changing roles, for example, and they spend less time on non-revenue-generating activities such as compliance-driven access reviews and approvals. As a result, these users can spend more time on core activities that create business value.

Exhibit 6:
Productivity: Horizons 3 and 4+ organizations are likely to see significant productivity gains



Source: SailPoint Customer Survey on IAM (n=227): Question 7.19 "How has the implementation of IAM automation use cases" (e.g., automated access provisioning, passwordless access, just in time access grant) affected the productivity of your front-line users?"

Organizations can leapfrog to Horizons 3 and 4 by adopting a unified approach across data, operations, and users, and deploying scalable solutions across on-premises, cloud, and hybrid environments. The benefits are substantial, including scaling identity security capabilities and lowering cyber risk without increasing the relative size of the IAM team.

Scalable identity security solutions are essential for organizations aiming to reach Horizons 3 and 4. These solutions should scale with growth in the number of identities governed, especially for machine identities, which survey results suggest have low levels of coverage today but will grow the fastest. With scalable solutions, organizations can maintain the effectiveness of their identity security measures as their digital ecosystems expand.

Investments in identity security are not a cost center—they are a strategic imperative that can yield disproportionately higher returns across risk reduction, productivity, and business value. Committed investments in identity security help organizations safeguard their assets and gain competitive advantages in the digital age.

Chapter 3:

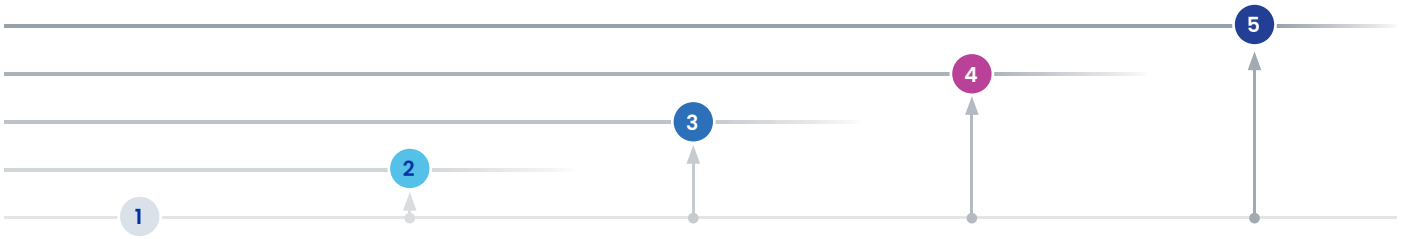
Where organizations are in their journeys and why mature organizations deliver higher returns?

The SailPoint Horizons maturity framework

SailPoint categorizes identity security programs into five maturity horizons based on an organization's maturity across four enablement areas: strategy, technology & tools, operating model, and talent.

Exhibit 7:

Over three years of annual surveys, we clustered key criteria into five 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

Highly automated capabilities with AI driving decisions based on risk estimations

Capabilities span across most identities (workforce, business network) and environments (data, cloud, APIs)

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

Identity team dedicated to identity innovation (i.e. Data scientist/ML specialist/ identity researchers) doing primary research and analysis, recognized as identity thought leaders

Extended and unified identity

Blurring boundaries between enterprise identity controls and external identity ecosystem

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

Technical capabilities support universal ID framework, dynamic trust model, identity integrated with security, frictionless access

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

Leverage support of developer community outside the boundaries of the organization

INSUFFICIENT	FOUNDATIONAL	ADVANCED

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

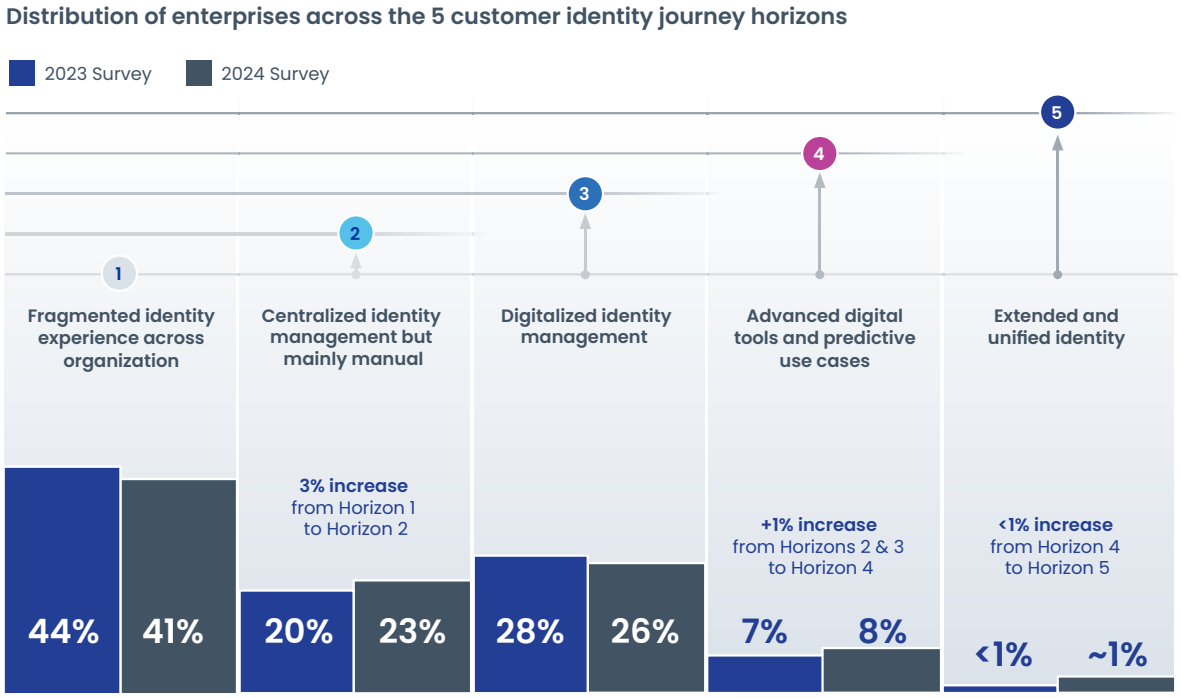
Based on interviews and a new survey of 350+ IAM decision makers across the globe, we explored where organizations stand in their identity security journeys and how they have progressed since last year. Our research helps explain why increasing identity security maturity yields disproportionately higher returns across risk reduction, business value, and productivity. Taken together, these perspectives illustrate where organizations have excelled, the barriers they face, and how they can move to the next maturity horizon.

Most organizations have only begun their identity security journeys

Despite some progress, most organizations remain in the early stages of their identity security journeys, including more than 40% still in Horizon 1, as shown in the exhibit [below]. Horizon 2 saw moderate growth in 2024, and some organizations moved from Horizon 3 into Horizon 4 by adopting a unified approach to identity security across environments and investing in leading-edge tools that generate actionable identity insights.

Exhibit 8:

With 41% of organizations still in Horizon 1, significant opportunity exists to unlock the "full potential" of identity security



Note: Horizon 1 is updated to include the unpenetrated IAM market (who are screened out of later sections of the survey)
Source: SailPoint Customer Survey on IAM (n=349); accounts for respondents that were terminated for not having a formal IAM program or deploying IAM tools

The slow pace of progress is due in part to pressure on cyber and IT budgets. In an era of cost-cutting, identity security professionals face challenges deploying and maintaining comprehensive identity security ecosystems. And almost every organization is finding it more difficult to attract and retain tech talent. That said, the slow but steady progress toward Horizon 4 and 5 indicates that organizations are finding ways to bolster their capabilities in pursuit of enhanced security and value to the business.

Slow but steady progress toward Horizon 4 and 5 indicates that organizations are finding ways to bolster their capabilities in pursuit of enhanced security and value to the business.

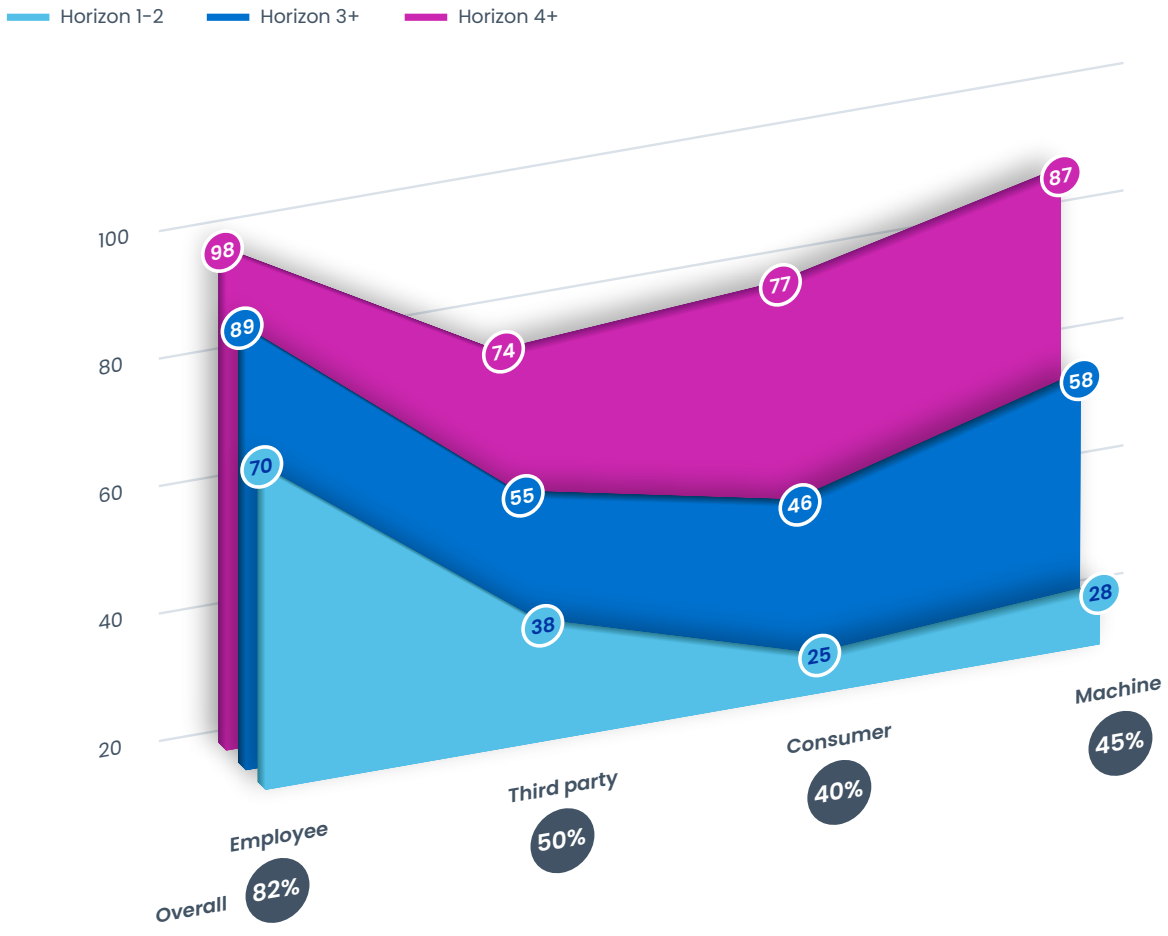
Organizations that invest in mature identity security see disproportionately higher returns because of unique capabilities across nine themes

Organizations with mature identity security share important characteristics, including higher security coverage of non-employee identities. By scaling their capabilities to address specific security needs for each identity type, organizations in Horizon 3 and beyond minimize vulnerabilities, detect and address high-risk account settings, and enhance overall security posture.

Exhibit 9:

Organizations at Horizon 4+ reduce risk with 70% capability coverage across identity types; Horizon 3 is close behind

Coverage across identity types
Share of respondents with average identity security capability coverage for each identity type

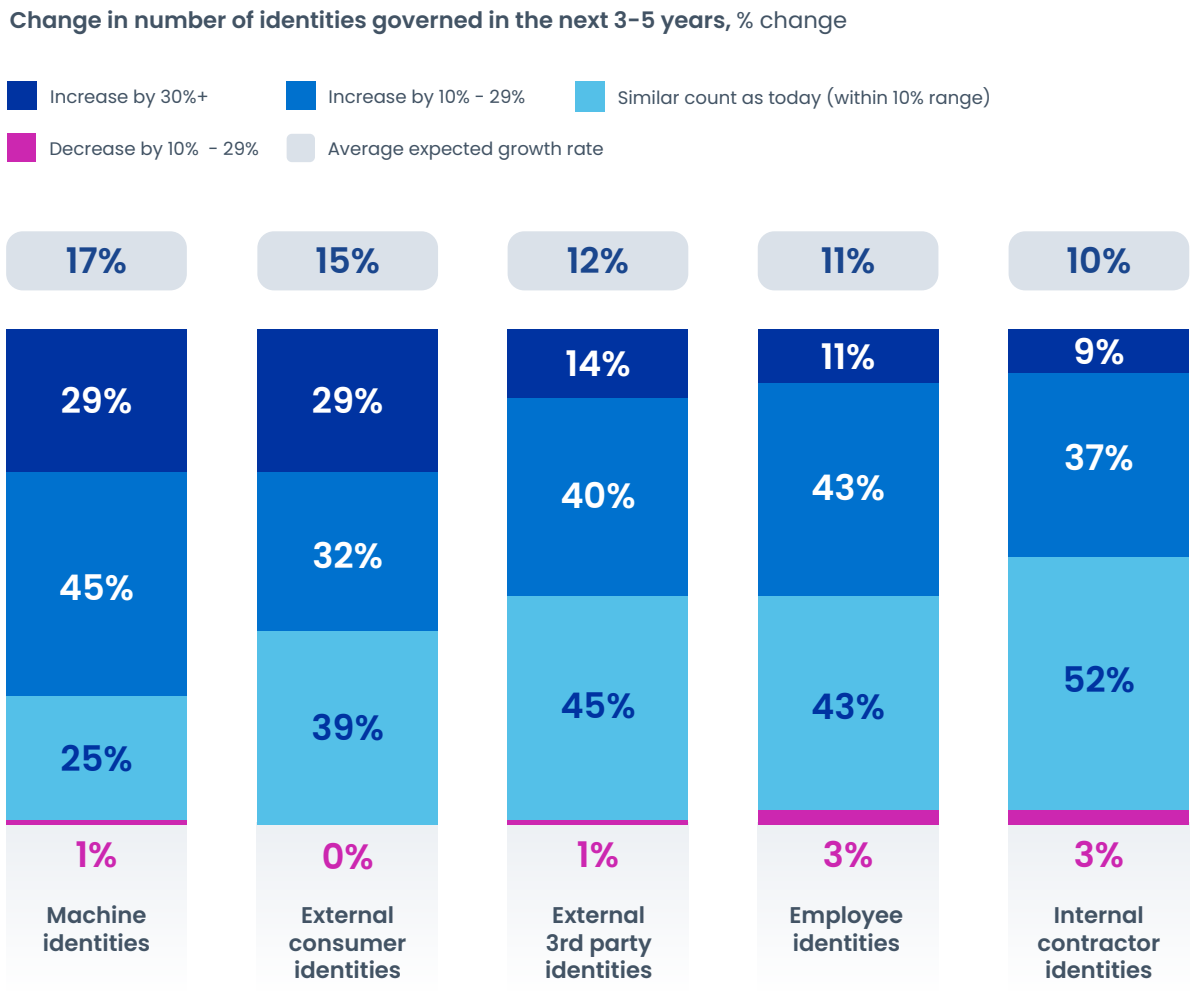


Source: SailPoint Customer Survey on IAM (n=227): Question 3.04 "Indicate whether your organization has already adopted the specific capability for each type of identity"

Horizon 3 and 4 organizations have scaled up coverage for machine identities in particular, while most in Horizons 1 and 2 remain focused on coverage for employee identities. With higher coverage across identity types, Horizon 3 and 4 organizations are in better positions to adapt to the ever-evolving threat landscape, where expanding identities and types present additional security risks.

Exhibit 10:

All identities are expected to grow roughly 14% in the next 3-5 years, with machine identities growing the fastest



Growth in machine identities may outpace growth in human identities

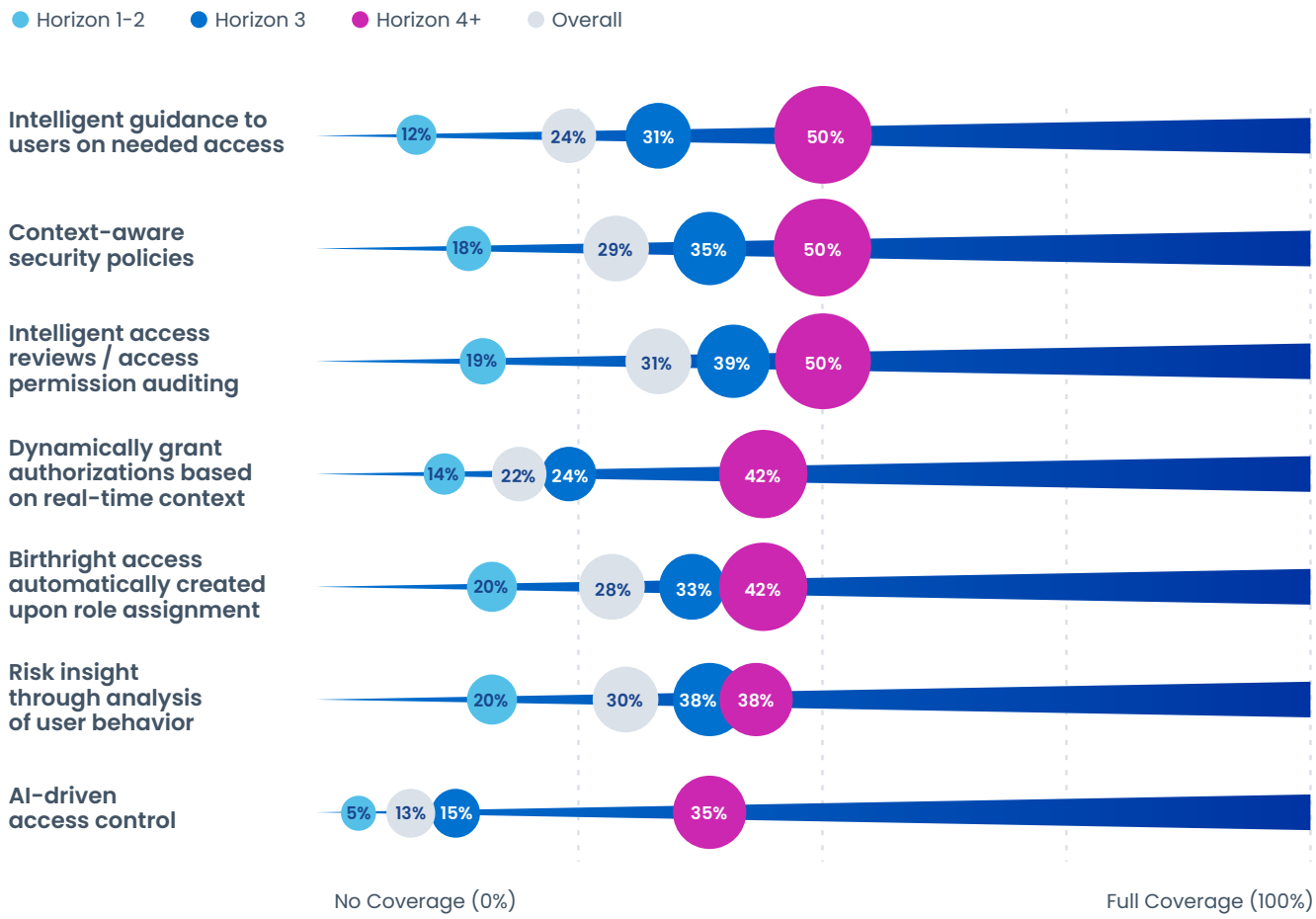
Source: SailPoint Customer Survey on IAM (n=227): Question 3.01 "What is the percent change in identities you expect your organization to govern in 3-5 years?"

Survey results show that machine identities are likely to grow faster than any other identity class, driven by expanding cloud workloads and AI use cases that require non-human account access. Given past survey results indicate machine identities already represent more than 40% of total identities within an organization, securing them will become even more critical to mitigate cyber threats. Horizon 1 and 2 organizations need to incorporate machine identities into their security roadmaps or risk falling behind.

Exhibit 11:

Horizon 4+ organizations are twice as likely to leverage identity data to create actionable intelligence and power new use cases

Adoption of identity data intelligence at scale, share of respondents



Source: SailPoint Customer Survey on IAM (n=227): Question 7.03A "How is your company harnessing its identity and access related data to create actionable intelligence?"

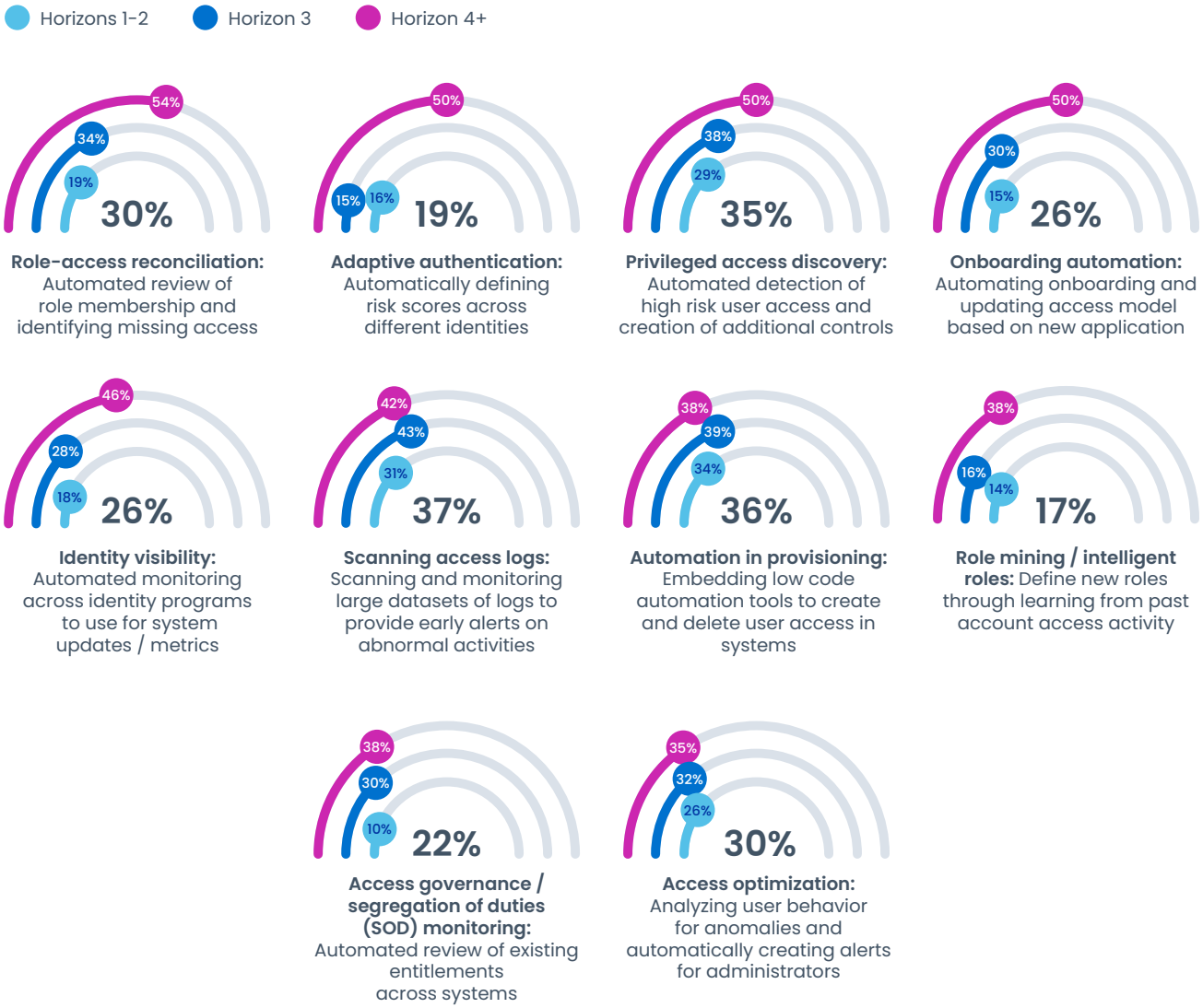
In addition to their higher coverage across identity types, organizations in Horizon 4 are significantly more adept at using identity data to create actionable intelligence and unlock additional value from their identity security investments. About 50% of Horizon 4 organizations use intelligent guidance for user access and intelligent access reviews, for example, compared to fewer than 40% of those in Horizon 3 and just 20% of those in Horizons 1-2.

More accurate and timely access decisioning, enabled by better use of identity data, is a key to reducing security risks. And significant productivity gains arise from streamlined access reviews and lower authentication friction. Horizon 4 organizations serve as a model for how organizations in Horizons 1-2 can harness identity data.

Exhibit 12:

Horizons 1-3 have low adoption of AI-powered use cases, suggesting significant opportunities

Top 10 AI-powered use cases by adoption, share of respondents



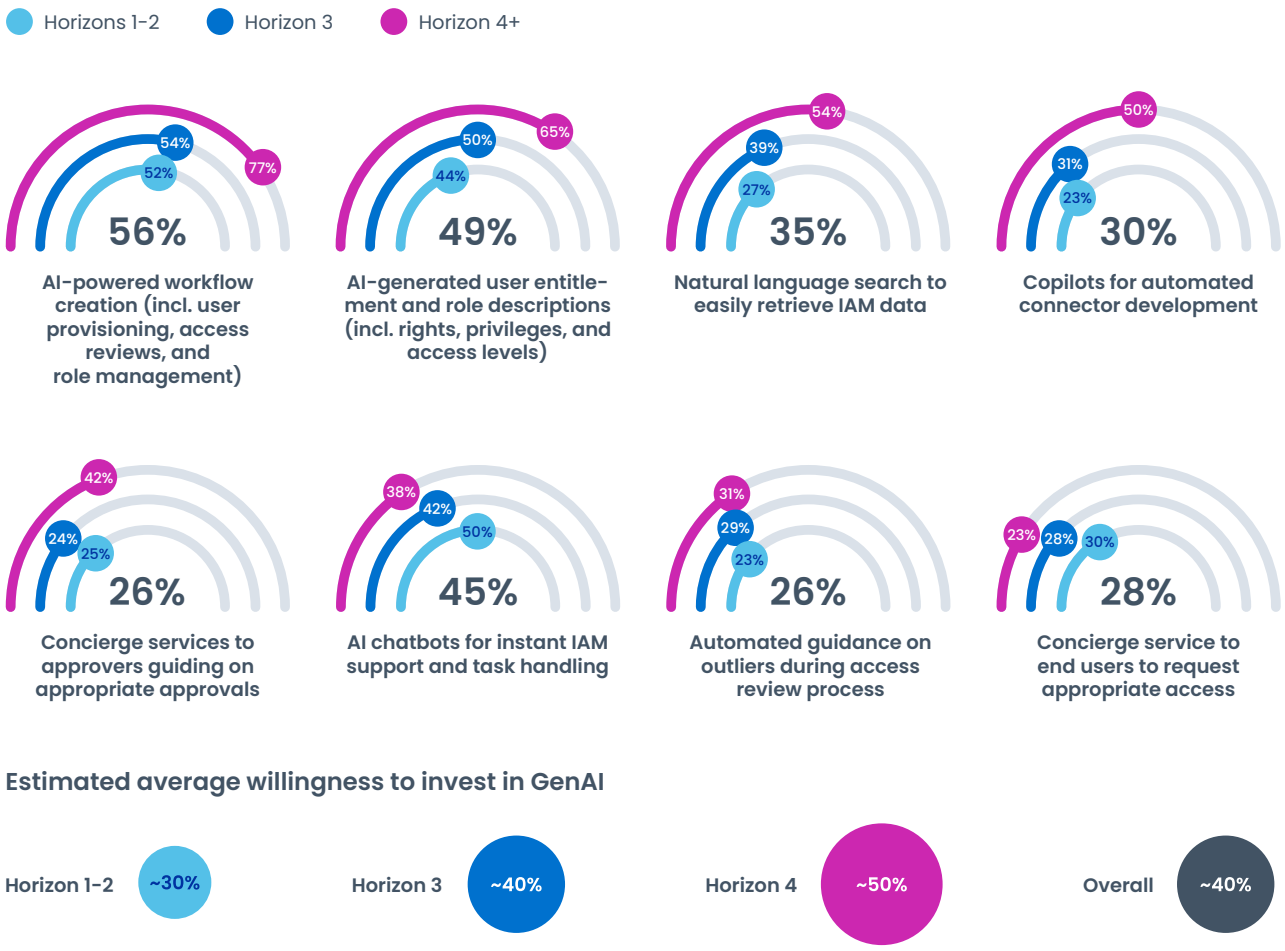
Source: SailPoint Customer Survey on IAM (n=227): Question 4.02 "Which of the following AI-powered use cases have you already implemented within IAM?"

Horizon 3 and 4 organizations are leading the way in adopting AI-powered identity solutions, with about 1.7 times higher adoption across use cases. Organizations with the highest identity security maturity have focused on adoption of AI for role-access reconciliation, adaptive authentication, and onboarding. These AI use cases drive improvements in front-line user productivity and lower costs with more efficient infrastructure maintenance and remediation, highlighting opportunities and incentives for lower-maturity organizations.

Exhibit 13:

Organizations with mature identity security have the foundations to invest in scalable GenAI-powered use cases

Willingness to invest in GenAI-powered use cases, share of respondents



Estimated average willingness to invest in GenAI

Source: SailPoint Customer Survey on IAM (n=227): Question 4.07 "Which of the following GenAI-powered use cases do you have already implemented or would be willing to invest in within IAM in the next 2-3 years?"

Beyond AI adoption, GenAI presents opportunities to create scalable solutions and enhance productivity, but only for organizations willing to invest. Horizon 3 and 4 organizations have the foundations to invest in scalable GenAI-powered use cases, prioritizing tools for workflow creation, user entitlements, role descriptions, and natural language search.

Most Horizon 1-2 organizations, on the other hand, remain focused on automating basic help desk activities, if they have begun considering GenAI in any form. While GenAI use cases may take time to develop, our research and experience suggest that they will yield disproportionate returns in productivity.

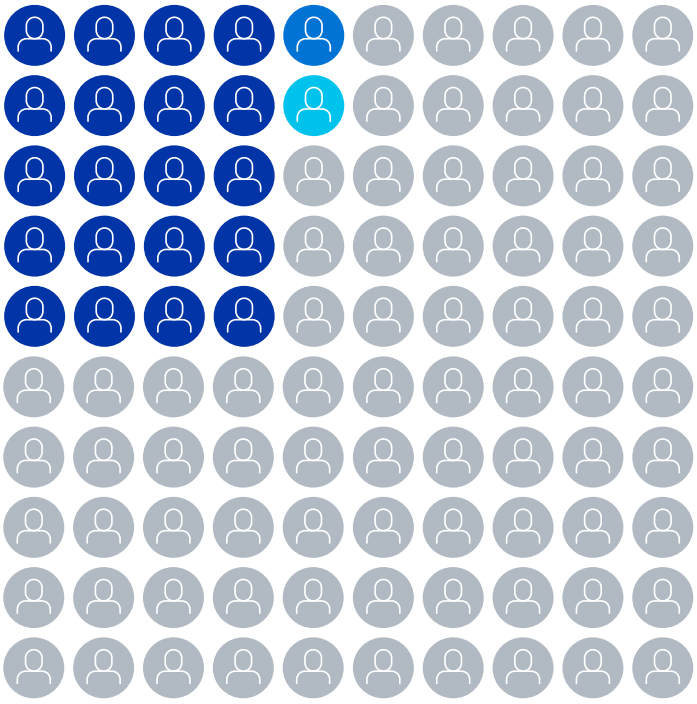
Exhibit 14:

Organizations can scale across Horizons with better capabilities and higher identity coverage without significantly larger IAM workforces

IAM specialist Other cybersecurity professional

Average size of IAM workforce as a share of overall cybersecurity workforce

Percent of IAM-specific employees (= 1%)



20–22%

of cybersecurity workforce is comprised of IAM specialists for Horizon 2+ organizations.

Note: While IAM specialists represent ~32% of cybersecurity workforce for Horizon 1 organizations, they represent 20–22% of Horizon 2+ cybersecurity workforce, likely driven by higher productivity

Source: SailPoint Customer Survey on IAM (n=227): Question 2.14 "How large is your cybersecurity workforce (including full time employees and contractors)?"; Question 2.15 "How large is your identity and access management (IAM) team (including full time employees and contractors)?"

As organizations add advanced identity security capabilities, they must build the right teams, both in size and skill, to manage identity security ecosystems. Horizon 1 organizations typically allocate about a third of their cybersecurity workforce to IAM, while organizations building more advanced IAM capabilities can scale from Horizon 2 to 3 and 4 without growing their IAM workforces as a share of overall cybersecurity professionals—doing more with the same resources.

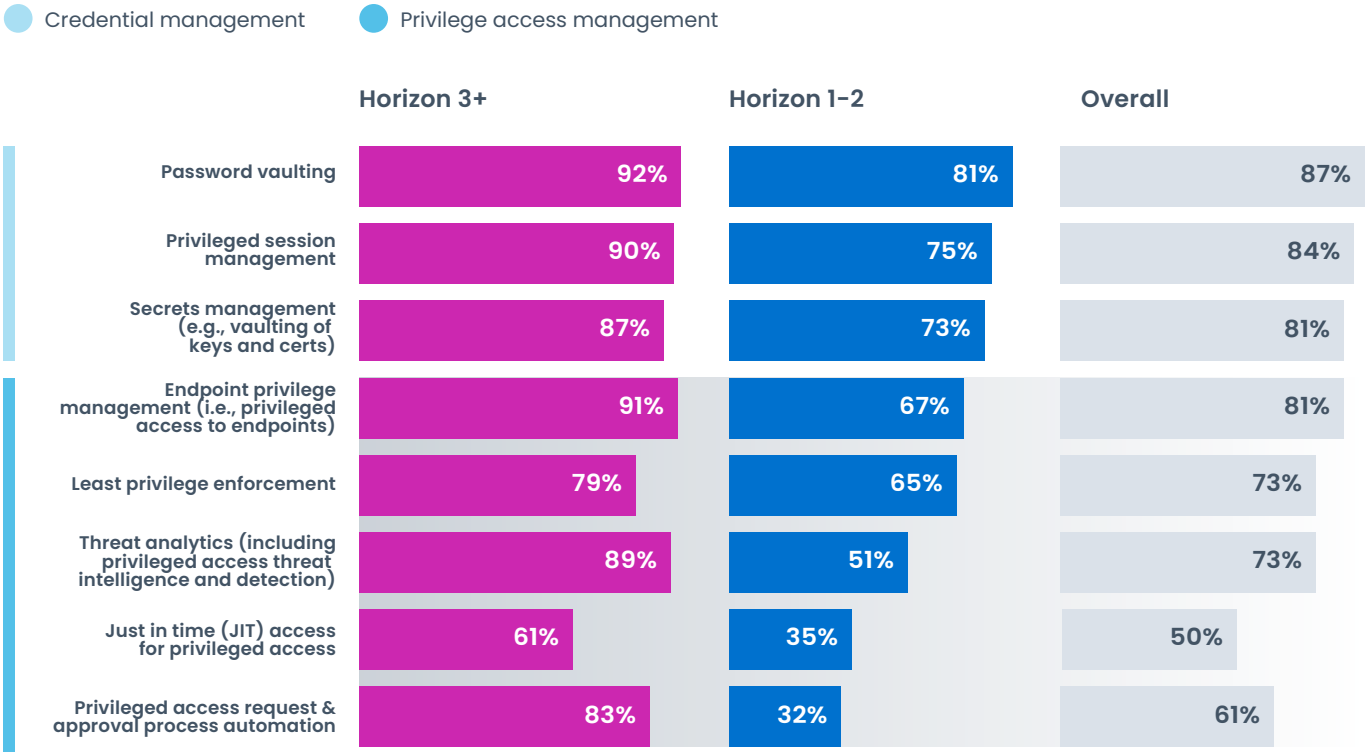
While advances in maturity may not require a larger IAM workforce, they do require changes in talent mix. Shifting from generalist IT support to engineering-led identity management is a critical step in transitioning to Horizons 3 and 4.

While advances in maturity may not require a larger IAM workforce, they do require changes in talent mix.

Exhibit 15:

Horizon 3+ organizations have up to ~50% higher adoption of privilege access governance capabilities as compared to Horizons 1-2

Adoption of PAM-specific capabilities by Horizon, % of respondents



Source: SailPoint Customer Survey on IAM (n=227): Question 3.03A "Which security capabilities has your organization adopted?"

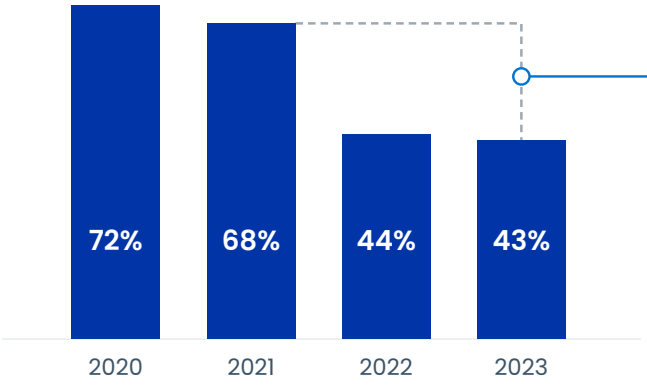
Adopting privileged access governance capabilities is essential to progress across horizons, and Horizon 3 and 4 organizations lead the way. While more than 80% of all organizations have implemented credential vaulting and session management, governance-specific capabilities have lower adoption rates, especially among Horizon 1 and 2 organizations. Horizon 3 and 4 organizations have 15-50% higher adoption across privileged access governance capabilities, highlighting substantial opportunities for lower-maturity organizations.

Exhibit 16:

As cyber insurers develop more mature ways to assess cyber risk management, cyber insurance premiums have risen

Cyber insurers have lowered their loss ratios and matured in assessing and managing risk...

Standalone cyber coverage loss ratios,
share of premiums paid out as claims

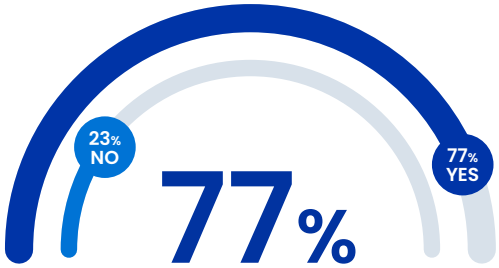


40%

Reduction in losses among cyber insurers indicates improved management of cyber risk

...and raised premiums to match heightened risk profile

Respondents who say premiums have risen in the past three years



77%

Organizations report premium increases
over the last 3 years

> **"Insurance companies are now drilling down more to see what security controls a company has ... they might incentivize you with discounts for implementing new security controls**
>
> Cyber insurance professional at major brokerage

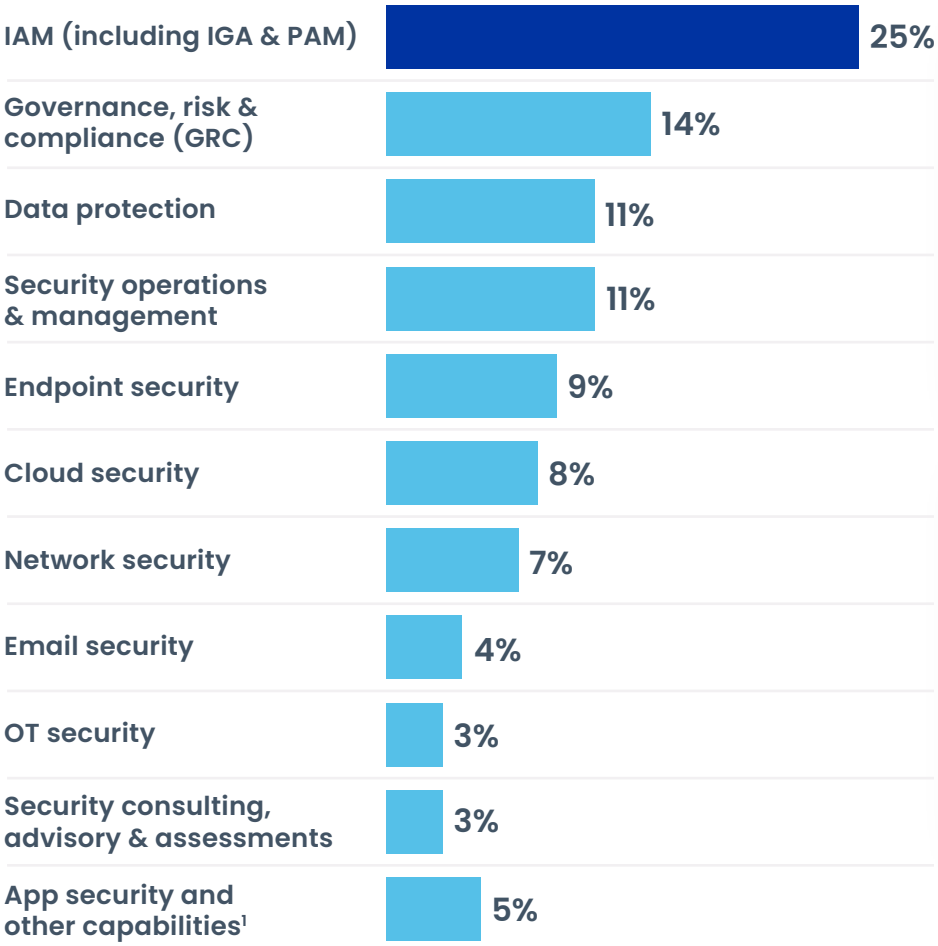
Source: Fitch Ratings; Expert interviews; SailPoint Customer Survey on IAM (n=227): Question 6.09 "What was the percent increase in your cybersecurity insurance premiums over the past 3 years?"

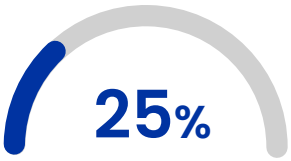
Enhanced identity security can help keep insurance premiums in check. Cyber insurers have been assessing cybersecurity risk more rigorously since 2020, reducing their losses by 40% despite the proliferation of threats. About 92% of survey respondents reported that carriers assess their cyber capabilities before setting premiums—and 77% are paying higher premiums. More mature organizations with lower risk profiles may have more leverage to slow premium growth.

Exhibit 17:

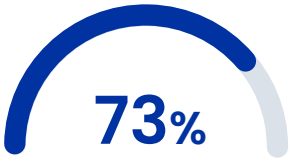
Cyber insurance customers report that identity security capabilities have the most impact on insurance assessments

Top cybersecurity capabilities impacting cyber insurance assessments
% of respondents who selected capability as the most impactful of all





25% of respondents consider IAM the most critical element in cyber insurance evaluations, the largest proportion



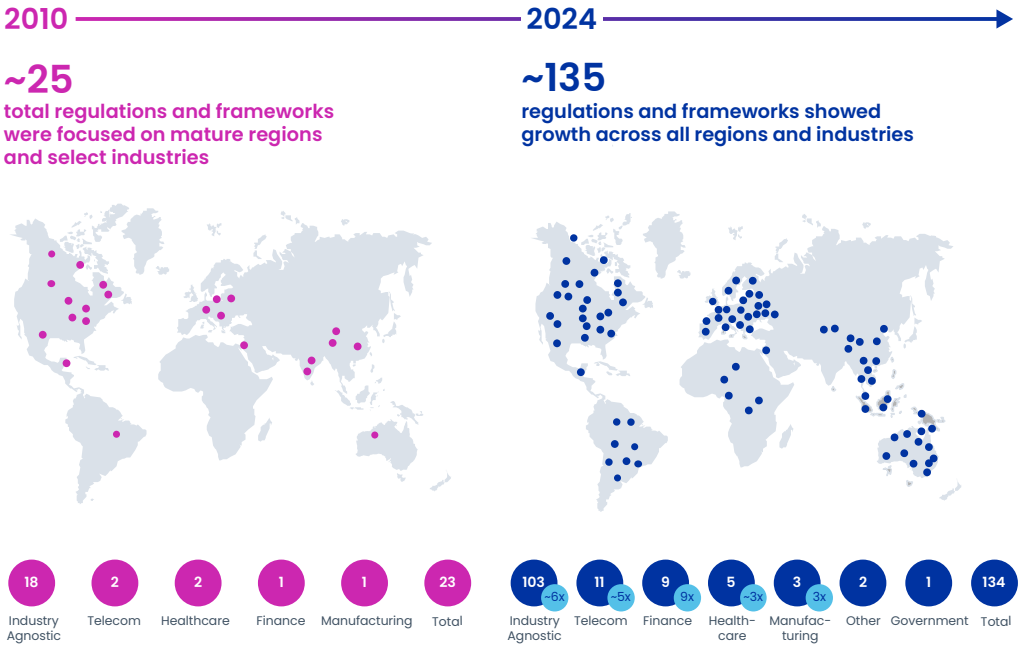
73% of cyber insurance customers consider IAM capabilities among the top three capabilities influencing insurance assessments

[1]Includes web security and MSSP / outsourcing
Source: SailPoint Customer Survey on IAM (n=227): Question 6.06 "If your company is assessed by your cybersecurity insurer to determine your cybersecurity insurance premium, rank the three cybersecurity capabilities that have impacted your assessment therefore premium the most?"

Of all security capabilities assessed by cyber insurers, IAM capabilities are considered the most critical in determining premiums. More than seven out of ten IAM decision-makers view IAM as one of the three most impactful security capabilities determining cyber insurance premiums, and a quarter view IAM as the single most impactful capability. This underscores IAM's critical role in managing both security and financial risks. We expect more organizations to invest in IAM capabilities to manage premium growth.

Exhibit 18:

Identity-related regulations have grown sevenfold since 2010 across regions and industries



IAM-related regulations have grown in density and complexity since 2010.

5x+ increase
in regulations of industries outside finance and healthcare

13x increase
in regulations outside North America, APAC, and Europe

Source: Press search

The regulatory landscape is evolving, with identity-related regulations growing sevenfold globally from 2010 to 2024. In 2010, there were about 25 major identity-related regulations, focusing mainly on specific industries in North America and Europe. This number has now ballooned to around 135 with substantial growth across regions and industries, raising compliance challenges.

As identity security regulations become more expansive and complex, the costs of falling out of compliance are rising; according to our survey, 74% of organizations facing identity-related compliance issues report remediation costs exceeding $1 million. Motivated by regulatory requirements and financial consequences, more organizations are turning to identity security solutions that simplify compliance and audit processes.

Across the board, we find that organizations seeing the biggest returns are investing in identity security with the aim of improving identity coverage and introducing automation. Organizations that understand both where they are today and what others have done to improve identity security are best equipped to overcome barriers to advancement. Whether an organization is stuck in Horizon 1 or has progressed to Horizon 4, strategic investment in identity security paves the way for secure and efficient business operations.

Chapter 4:

How leading organizations are bending the curve?

Around the world and across industries, leading organizations are now investing in identity security to bend the curve, delivering outsized returns in compliance, operational efficiency, user productivity, and security.

In this chapter, we provide case studies in two categories: one covers the three facets of bending the curve, and the other shows how organizations leapfrog horizons to counter cyber threats while gaining competitive advantages and controlling costs.

Exhibit 19:

Goal	Solutions and results
Reduced cyber risk	**Currys, a UK-based tech retailer with over 800 stores, reduced its risk profile by enhancing identity governance and automating identity security.** Its previous approach, using Excel-based manual processes with a constantly shifting pool of employees, led to over-provisioning and compliance risks. Automation now provides a complete audit trail, minimizing compliance challenges and non-executed permissions while strengthening overall security posture.
Higher business value	**Absa, a pan-African financial institution with more than 35,000 employees, streamlined onboarding and third-party identity management while lowering costs.** To comply with GDPR and POPIA, the bank deployed an AI-based risk management tool with just-in-time provisioning and standardized certification for third-party identities. This risk-based access model has lowered operational overhead and simplified identity governance for contractors and non-employees.
Productivity	**Merck, a leading pharmaceutical company with 72,000 employees, enhanced productivity and efficiency by automating IAM tasks.** The company sought a scalable, cloud-based system to replace its dated on-premise identity solution, which required significant manual maintenance. By onboarding a new cloud-based system, Merck simplified regulatory compliance and achieved notable reductions in time spent on access reviews and waiting for access.
	BNP Paribas Bank Polska boosted productivity with extensive automation of manual IAM tasks. Following a series of mergers, the bank was managing 10,000 users and about 1,000 applications through disjointed IAM programs. Without automation, the IT team was unable to cope with the volume of user requests or IAM tasks. With automation, all certification campaigns are now managed by just two employees, each allocating only about 15% of their worktime.

3x risk reduction by setting appropriate privileges for about 6,000 accounts	**210** hours of manual effort saved annually	**24k** identities managed
$300 savings per identity onboarded	**15** day reduction in onboarding time for 3rd party identities	**12k** non-employees empowered with secure identities
40% reduction in time spent on access reviews	**20%** reduction in time spent waiting for access	**30%** reduction of manual tasks performed by IT operations
40k automated identity tasks executed monthly	**90%** of access requests executed automatically	**4k** automated resets and password changes monthly

Exhibit 20:

A global technology group leapfrogged from Horizon 1 to Horizon 3+ over 24 months with a "Great Transformation" initiative

Horizon 1 (2020)	Horizon 3+ (2022)	Actions
0 formal identity and access management processes	**1** unified identity and access management program governing all staff accounts	**Established organization-wide identity strategy and call to action** informed by in-depth, independent cybersecurity gap analysis
21 days to deactivate and 5 days to activate user accounts	**0** wait time with instantaneous provisioning and deprovisioning	**Automated account provisioning and deprovisioning,** boosting the productivity of system administrators and freeing them to do more strategic work
<5 business units with centralized identity governance	**47** business units with centralized governance of about 23,000 application accounts	**Centralized identity governance processes across business units** through cloud-based identity platform that scales easily as the number of identities grows
<1k accounts managed through automated processes	**144k** automated account modifications and verifications	**Deployed advanced risk assessment applications** to dynamically update access privileges, reducing potential security threats

> **"We were starting from zero. But this gave us the opportunity to leapfrog using technology. We made the call to invest time and effort into the organization's most valuable asset: the identity.**
>
> **CISO,** Aboitiz Equity Ventures

aboitiz

Exhibit 21:

RWE leapfrogged from Horizon 2 to Horizon 4 in just six months with an identity-first IT transformation

Horizon 2	Horizon 4	Actions
On-premise, manual identity management processes	**Cloud, AI-driven** solution with identity security at scale	**Transitioned to cloud-based identity management,** cutting per-user provisioning expenses and eliminating the need to manage underlying architecture
2.5k user accounts	**~30k** user accounts	**Adopted AI-access modeling and access recommendations** to dynamically maintain and update functional group entitlements
0 business units with unified identity strategy	**30** business units sharing a unified identity strategy	**Scaled identity governance to all business units,** using dashboards to visualize JML metrics and provide actionable identity insights
25 days of onboarding lead time	**<3** hours of onboarding lead time	**Streamlined onboarding processes organization-wide,** using automation to enable self-service and eliminate ad hoc methods of identity provisioning

> **The migration made a huge difference from a cost and support perspective...freeing us to focus our operational efforts elsewhere. And users saw no difference at all.**
>
> **Cybersecurity manager,** RWE

RWE

Chapter 5:

Your path to the next horizon

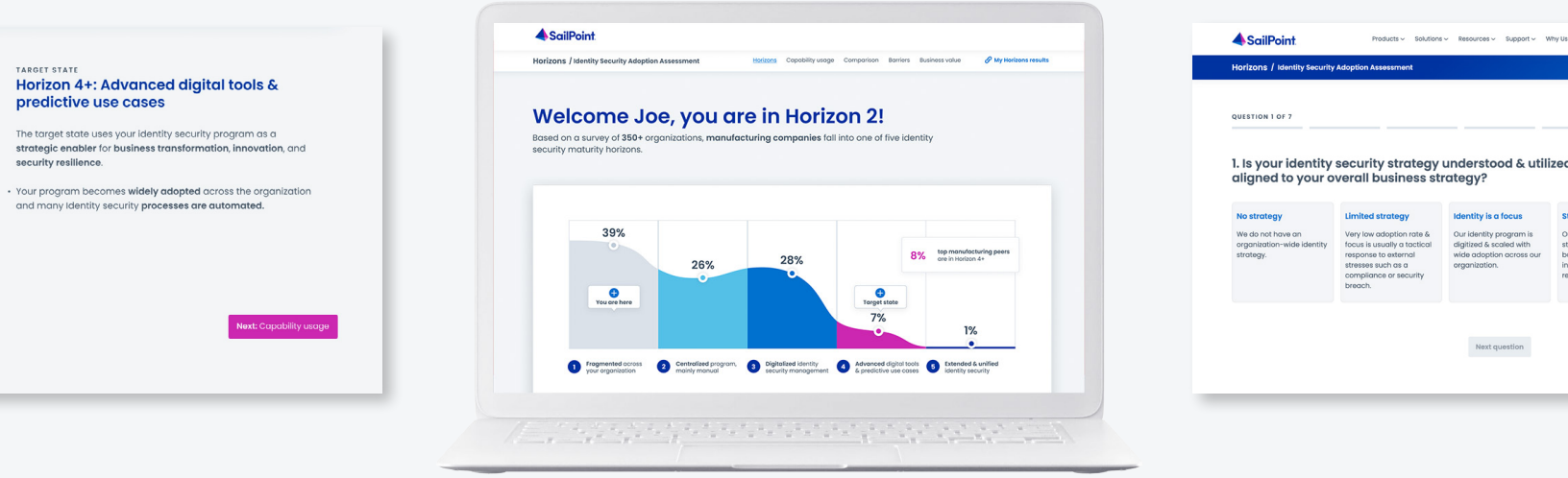
As cyber threats and regulatory demands intensify, committed investment in identity security is no longer optional—it's a strategic imperative. Investing to reach mature identity security horizons can bend the curve, reducing cyber risk while increasing business value and productivity.

Simply adopting new tools is not enough however. Harnessing the full power of identity requires a unified approach across data, operations, and users, and scalable solutions across environments. The journey has six main steps:

1. **Set a north star vision** for the identity security strategy, informed by trends shaping the future of identity security and the maturity of your program today.
2. **Invest in identity security solutions, especially AI-enabled solutions,** that will enable you to leapfrog horizons and deliver disproportionately higher returns.
3. **Consider a holistic approach to secure all types of identities** within the organization i.e. employees, third parties, and non-human or machine identities.
4. **Integrate IAM with broader security operations** to enable continuous monitoring, accelerate incident response, and control cyber insurance premiums.
5. **Leverage identity data to derive actionable insights,** improve access decisions, and create adaptive security policies.
6. **Stay ahead of emerging identity security regulations and standards** to maintain compliance and strong governance.

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.



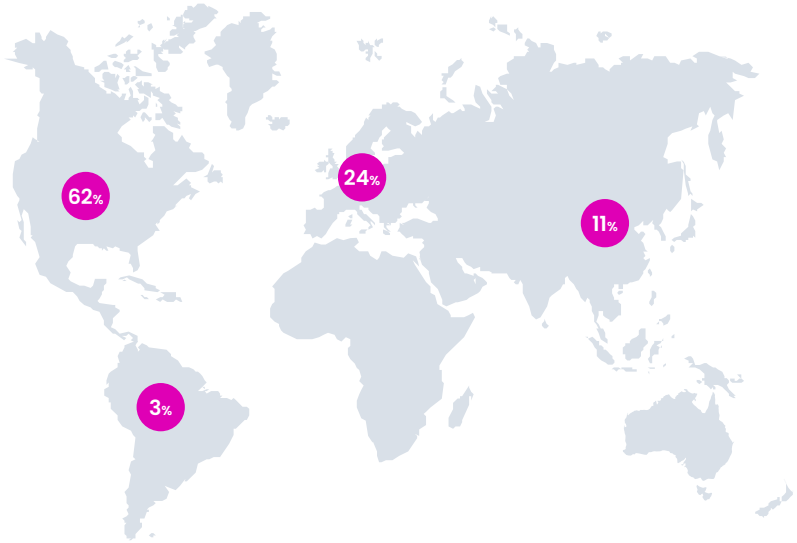
Appendix

Approach, methodology, and demographics

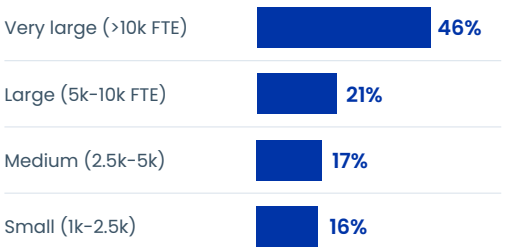
The insights in this report are based on a July 2024 survey of nearly 350 cybersecurity executives across North America, Latin America, Asia, and Europe, supplemented with interviews of IAM experts.

We surveyed 349 IAM decision-makers across the globe

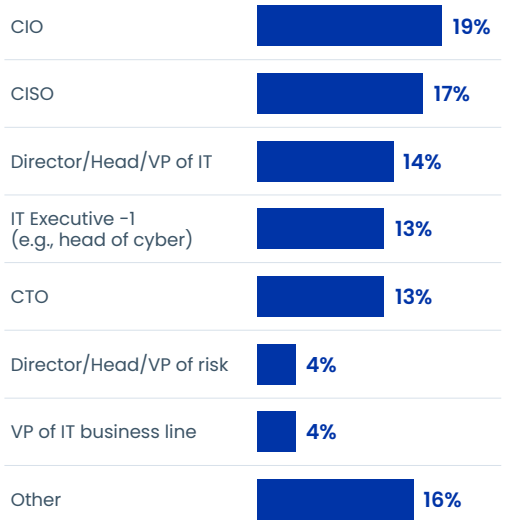
Geo Headquarter breakdown (n=349)



Firm size breakdown (n=349)



Decision makers include (n=349)



Respondents came from these industries

27% Financial services	**4%** Communications & media services	**5%** Government	**11%** Manufacturing
15% Healthcare	**19%** Technology	**4%** Utilities	**15%** Other

Note: Completed response pool (n=227) is source for all data cuts except horizon distribution; Total response pool (n=349) is source for horizon distribution (accounts for respondents that were terminated for not having a formal IAM program or deploying IGA tools)

The survey included several questions from 2022 and 2023 surveys to classify organizations into horizons using a consistent methodology.

The 2024 survey queried respondents regarding their adoption and use of 53 IAM capabilities across identity types, data, applications, and infrastructure. We also asked about the barriers they face and the time they needed to scale adopted capabilities.

Sources

[U.S.] National Cyber Strategy, March 2023: **https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf**

2024 Report on the Cybersecurity Posture of the United States, May 2024: **https://www.whitehouse.gov/wp-content/uploads/2024/05/2024-Report-on-the-Cybersecurity-Posture-of-the-United-States.pdf**

"From Data Chaos to Cohesion: How OCSF is Optimizing Cyber Threat Detection," AWS, Aug 5, 2024: **https://aws.amazon.com/blogs/opensource/from-data-chaos-to-cohesion-how-ocsf-is-optimizing-cyber-threat-detection/**

"CISA Establishing New Office Focused on Zero Trust," FedScoop, Feb. 15, 2024: **https://fedscoop.com/cisa-zero-trust-initiative-office-sean-connelly/**

Veriff Fraud Industry Pulse Survey - Key Findings, June 18, 2024: **https://www.veriff.com/fraud/news/veriff-fraud-industry-pulse-survey-key-findings**

"Identity & Access Forum Launches Industry's First Template for Building Mobile Driver's License Use Cases," Secure Technology Alliance, April 17, 2024: **https://www.securetechalliance.org/identity-access-forum-launches-industrys-first-template-for-building-mobile-drivers-license-use-cases/**

"Eid European Digital Identity (eID): Council Adopts Legal Framework on a Secure and Trustworthy Digital Wallet for all Europeans," Council of the European Union press release, March 26, 2023: **https://www.consilium.europa.eu/en/press/press-releases/2024/03/26/european-digital-identity-eid-council-adopts-legal-framework-on-a-secure-and-trustworthy-digital-wallet-for-all-europeans/**

"What Leaders Need to Know About the Australian Digital ID Bill 2024," Forbes, May 25, 2024: **https://www.forbes.com/sites/benjaminlaker/2024/05/25/what-leaders-need-to-know-about-the-australian-digital-id-bill-2024/ https://www.forbes.com/sites/benjaminlaker/2024/05/25/what-leaders-need-to-know-about-the-australian-digital-id-bill-2024/**

"Microsoft, Google do a Victory Lap around Passkeys," The Register, May 2, 2024: **https://www.theregister.com/2024/05/02/microsoft_google_passkeys/**

"Delta Expands Digital ID Program to LAX, LGA and JFK for Touchless Airport Experience," Delta News Hub, Dec. 12, 2023: **https://news.delta.com/delta-expands-digital-id-program-lax-lga-and-jfk-touchless-airport-experience**

[E.U.] AI Act, March 2024: **https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai**

"India Passes Long Awaited Privacy Law," WilmerHale, Aug 18, 2023: **https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20230818-india-passes-long-awaited-privacy-law**

NIST Security Framework 2.0, National Institute of Standards and Technology, Feb. 26, 2024: **https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf**

"The SEC's New Cybersecurity Disclosure Rules Decoded: What They Mean for Investors," Reuters, May 31, 2024: **https://www.reuters.com/legal/legalindustry/secs-new-cybersecurity-disclosure-rules-decoded-what-they-mean-investors-2024-05-31/**

"Proposed Rule Issued to Implement Cyber Incident Reporting for Critical Infrastructure Act," Mayer Brown, March 29, 2024: **https://www.mayerbrown.com/en/insights/publications/2024/03/proposed-rule-issued-to-implement-cyber-incident-reporting-for-critical-infrastructure-act**

"U.S. Cyber Insurance Maintains Strong Profits; Premium Growth Slows," Fitch Ratings, April 16, 2024: **https://www.fitchratings.com/research/insurance/us-cyber-insurance-maintains-strong-profits-premium-growth-slows-16-04-2024**

Select case studies: **https://www.sailpoint.com/customers**

About SailPoint

SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

sailpoint.com

SP2487-2409