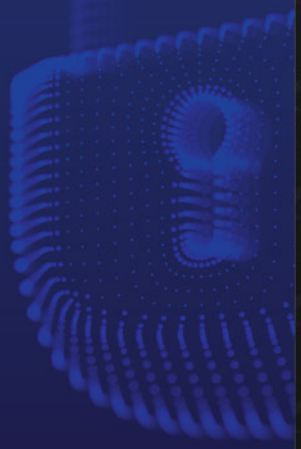
ManageEngine
PAM360

Identity Security Outlook 2026

A security leader's pulse on identity security investment priorities, emerging trends, and strategic imperatives for 2026 and beyond



ManageEngine
PAM360

TABLE OF CONTENTS

Executive summary

Identity security in 2026 will be shaped by three forces: the relentless growth of non-human identities that demand governance at scale, the natural progression into unified IAM operations, and the measured implementation of artificial intelligence (AI) to augment and complement what security teams can accomplish. Organizations that recognize consolidation as the foundation for managing complexity, not just reducing costs, will be positioned to build the resilient identity architectures the next decade demands.

For boards and executive leadership, identity security has moved from an operational requirement to a core enabler of business continuity. The question is no longer "Are we compliant?" but "Can our identity architecture support our pace of growth without amplifying risk or operational strain?" The organizations answering "yes" are those investing in architectural simplicity over expanding tool sets, building governance models that scale with non human identity growth, and adopting AI-enabled identity orchestration to reduce friction and improve confidence in decisions. They view modernization and consolidation not as budget exercises, but as strategic commitments to resilience, clarity, and long-term identity integrity.

Ramanathan Kannabiran,
director of product management
at ManageEngine

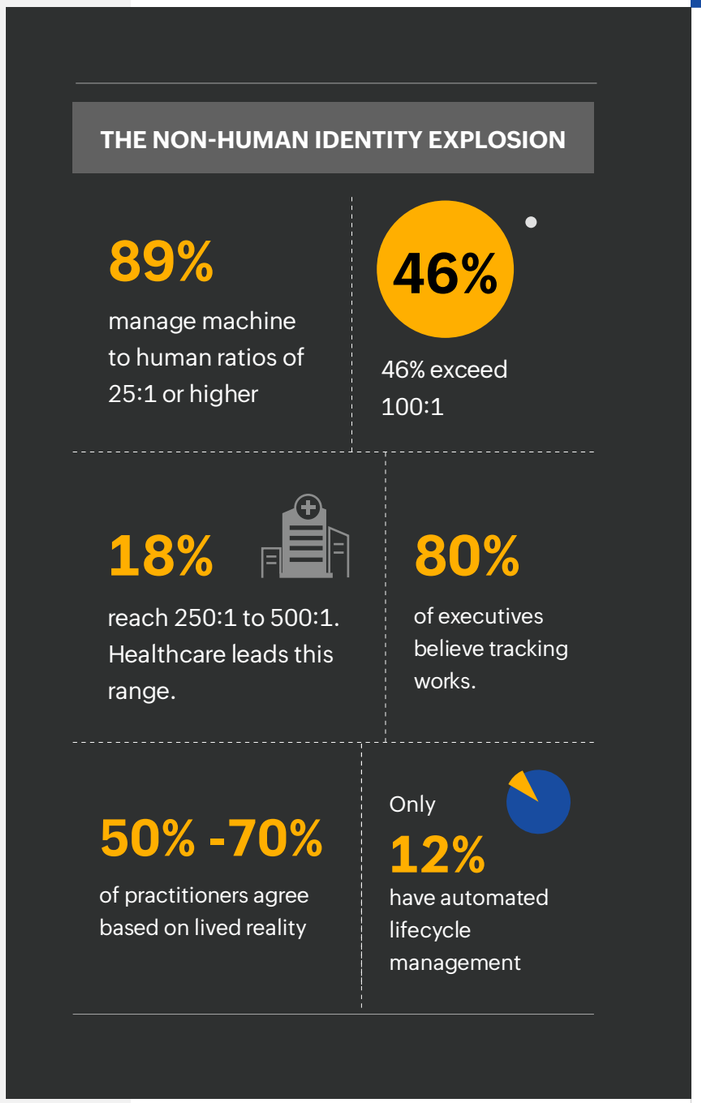
Identity security stands at a critical juncture. The convergence of three forces—explosive growth in non-human identities (NHI), rapid AI adoption, and unsustainable vendor fragmentation—is compelling security leaders to make architectural decisions that will define their organizations' security postures for the next decade.

This report presents findings from 515 senior identity and security professionals across the United States and Canada. With 54% holding director-level or above positions, 51% representing enterprises with over 250 employees, and 57% from organizations exceeding $100 million in annual revenue, this research captures the strategic thinking of leaders who control identity security budgets and set organizational direction.

This leadership-heavy research provides insight into strategic thinking at the highest levels of identity security decision-making while also capturing the operational realities faced by practitioners managing these systems daily.

Security leaders will use this research to:

- Benchmark their identity security maturity against industry peers.
- Build business cases for consolidation that resonate with CFOs and executive boards.
- Establish concrete intervention thresholds for machine identity governance.
- Sequence AI adoption to maximize value while minimizing premature deployment risk.
- Align budget allocation with the challenges most likely to impact security outcomes.



Top stories anchoring this report

1

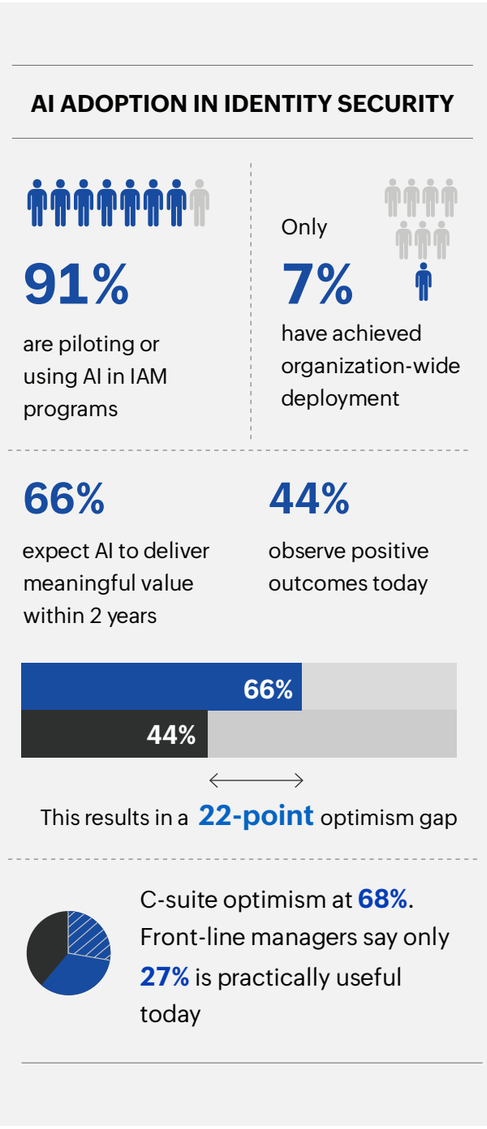
The NHI explosion

North American enterprises now manage at least 100 times more machine identities than human identities, with some sectors reaching a ratio of 500:1. This astronomical rise signals that the next wave of identity security will be defined by NHIs, not humans.

2

AI in identity security: *More promise than proof*

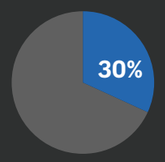
While 91% of organizations are piloting or using AI in IAM operations, only 7% have achieved organization-wide deployment. A 22-point optimism gap exists between future expectations (nearly 66% of AI users are confident about AI's future value) and current outcomes (almost 44% of AI users are seeing positive outcomes now).



THE IDENTITY STACKS OF TODAY

74%

operate with 2 or more identity vendors



Only

30%

use a single consolidated vendor

1 in 3

spend more time managing vendors than users

TOP PAIN DRIVERS:

40.7%	Cost
37.4%	Skills shortages
34%	Integration issues

Complexity spikes once a second system is added. It does not rise gradually

3

The identity security stack is fragmented by design

Nearly three in four organizations operate with multiple IAM vendors, and one in three spend more time managing vendors than managing privileged users. Complexity spikes early, not gradually.

4

Consolidation is no longer a debate

76% of North American firms are either consolidating or evaluating vendor unification. Resistance is virtually non-existent. The question has shifted from “Should we?” to “How quickly can we execute?”

5

Budgets are recalibrating, not shrinking

Over 92% of respondents expect identity security budgets to grow or remain stable. Among the minority anticipating cuts, 60% attribute them to consolidation efficiencies strategic optimization.

BUDGETS STAY STRONG

92%

expect budgets to stay stable or grow

66%

anticipate increases

Among those cutting, **31%** attribute savings to consolidation efficiency

TOP SPENDING PRIORITIES:

41%	Integration
43%	AI
40%	Zero Trust
36%	NHI security

Consolidation ranks at **21% to 24%** depending on organization type

CONSOLIDATION MOMENTUM IS REAL

76%

are consolidating or actively evaluating

Only **27%**

are currently in transition

support consolidation	73%
strong support	32%
moderate	41%

0.28% have no consolidation plans

TOP DRIVERS:

61%

Cost reduction

46%

relief from operational chaos

6

The 2026 outlook

Organizations in 2026 are aiming for consolidation for unified control and AI for continuity and modernization. The most defining force shaping identity security isn’t AI; it’s the shortage of skilled practitioners needed to manage increasingly complex ecosystems.

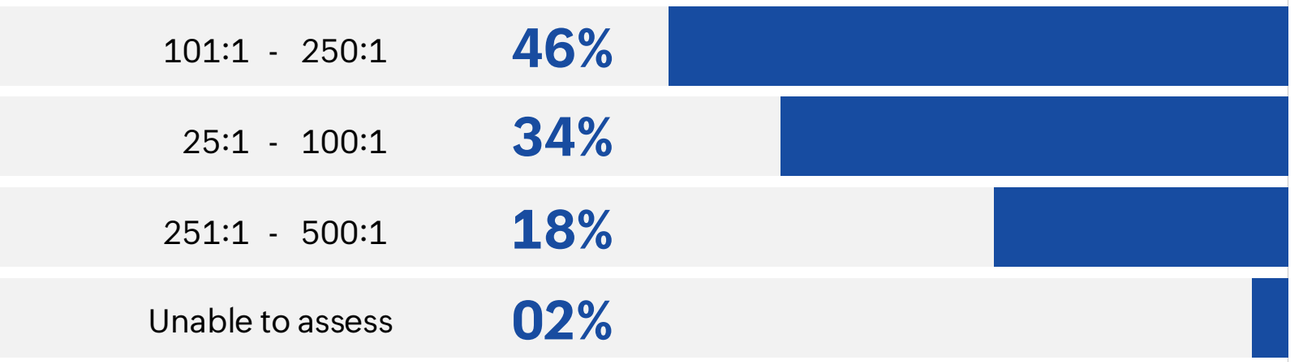
The NHI crisis:

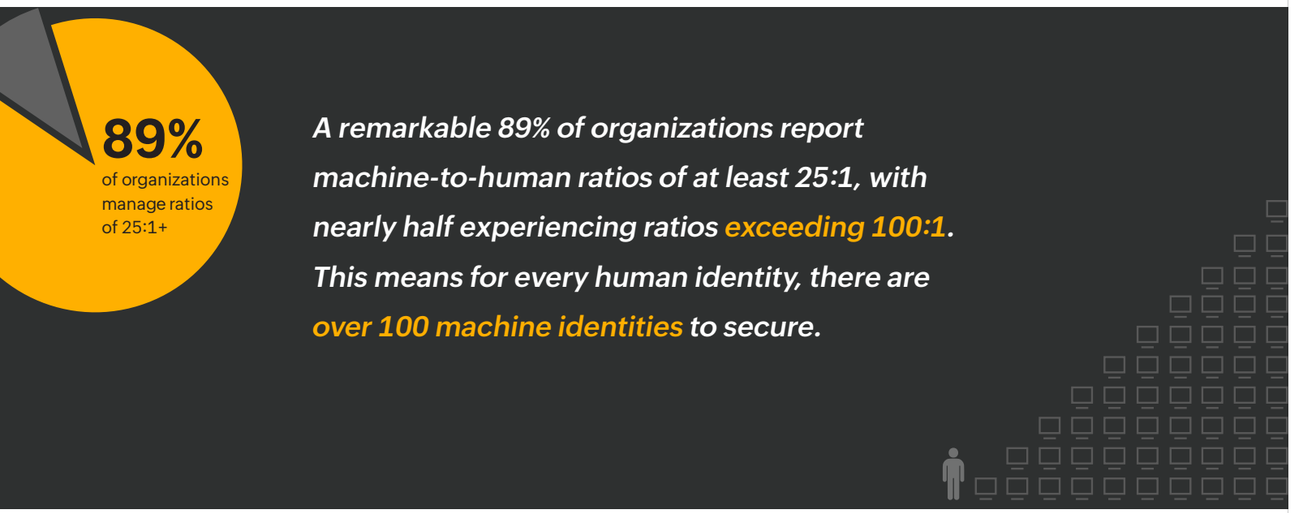
1

Securing the invisible

The challenge with the NHI scale

The survey's most striking finding concerns the ratio of machine identities to human identities within organizations. Machine identities, such as service accounts, API keys, bots, agents, and certificates, have proliferated as organizations embrace automation, cloud services, and DevOps practices.





The visibility paradox:
Dissonance between leadership perception and operational reality

While 80% of top leaders believe dormant or orphaned machine accounts are tracked, barely 50–70% of practitioners confirm it. This perception gap reveals a widening chasm between strategic assurance and operational reality.

This visibility gap stems from multiple sources: legacy systems lacking modern integration capabilities, decentralized IT environments from merger and acquisition activity, and the sheer velocity of NHI creation outpacing governance processes.

Where's the disconnect?

The disconnect stems from multiple root causes that compound each other:

It's a reporting problem

Dashboards and reports presented to executives often aggregate data in ways that obscure gaps rather than reveal them. A report showing that 80% of machine identities are tracked sounds reassuring but masks critical details. That remaining 20% might include the most privileged service accounts with access to

production databases, financial systems, or customer data. These metrics emphasize coverage percentages without contextualizing risk concentration. Executives see green check marks indicating "tracking implemented" without understanding that "tracking" might mean "we know it exists" rather than "we actively monitor and govern it."

It's a tool problem

Many organizations deploy identity governance platforms that excel at managing human identities but lack comprehensive discovery capabilities for machine identities across hybrid infrastructure. Traditional IAM tools were designed when machine identities were a small fraction of total identities. They struggle to discover service accounts in cloud environments, API keys embedded in code, certificates distributed across containers, and bot accounts operating autonomously. The tools executives believe provide complete visibility actually provide partial coverage, creating false confidence.

It's a cultural disconnect

Executives focus on compliance checkboxes, audit readiness, and board-reportable metrics. Practitioners understand that "tracked" doesn't mean "secured" or even "actively monitored." The cultural gap between "we have a tool that can track" (executive understanding) and "we actively govern all identities" (operational reality) creates persistent misalignment. Executives interpret capability as implementation; practitioners know capability doesn't equal operational maturity.

There's something more fundamental

Machine identity management lacks clear executive ownership in most organizations. Machine identities fall into the gaps between infrastructure teams (who create service accounts), development teams (who generate API keys), security teams (who should govern them), and operations teams (who maintain them). Without clear ownership, accountability diffuses.

Innovation turns into entropy when scale exceeds control

The proliferation of machine identities stops being a sign of innovation the moment an organization can no longer map, monitor, or meaningfully govern them. It becomes a systemic risk when machine identities begin operating as invisible actors inside the environment.

A single unused API key with elevated permissions. A forgotten service account tied to a deprecated workflow. A container spawned at build time that still retains production access long after shutdown. When the organization can no longer ensure that every machine identity maps to a legitimate purpose, life cycle, and permission boundary, the identity layer itself becomes a silent vulnerability. At that point, the innovation that enabled speed now fuels risk at scale.

The survey data suggests organizations should consider mandatory life cycle controls when:

- → **Orphaned/dormant accounts exceed 25%** of total machine identities.
- → **Machine-to-human ratios surpass 100:1** without commensurate automation in life cycle management.
- → **More than 25% of the IAM team's time** is spent on integration maintenance rather than security operations.

Only 12% of organizations have achieved comprehensive automated life cycle management for machine identities.

The remaining 88% rely on manual or ad-hoc processes that cannot scale with 100:1 ratio. This creates a mounting inventory of unmonitored attack vectors: each orphaned service account and each forgotten API key representing a potential breach pathway.

When organizations have more NHIs than they can reasonably govern

From access management to risk management

Traditional identity governance asks “Does this identity have appropriate access?” When managing 500 machine identities per human with traditional tools, this question becomes operationally impossible to answer for each identity. The paradigm must shift to “Do we understand the blast radius if this identity is compromised?” and “Can we detect anomalous behavior at scale?” Organizations must move from preventive access review to detective risk management, because prevention doesn’t scale to these volumes.

From human-centric to identity-agnostic security

Security models, policies, controls, and monitoring tools were all designed assuming the user is human. At 100:1 or 500:1 ratios, this assumption breaks. Machine identities don’t log in from office locations during business hours. They don’t forget passwords. They don’t fall for phishing. They behave differently, authenticate continuously, and operate at speeds and scales that human-centric security models cannot accommodate. The entire identity security framework must evolve to be identity-type agnostic.

From manual to automated governance

Human-in-the-loop processes like periodic access reviews, manual certification campaigns, and approval workflows cannot function at 100:1 scale. A team of 10 IAM administrators managing identities for 10,000 employees (1000:1 ratio) faces 1 million machine identities at a 100:1 machine-to-human ratio. Manual governance becomes mathematically impossible. Automation, continuous monitoring, and policy-driven controls transition from operational efficiency improvement to existential necessity.

From a static to dynamic life cycle

Human identities have relatively stable life cycles measured in years: onboarding, role changes, offboarding. Machine identities should have dynamic life cycles measured in hours or days: created for specific tasks, used, and destroyed. But without automated life cycle management, machine identities persist indefinitely, because there’s no HR offboarding trigger and no manager notification when they’re no longer needed. Organizations must implement time-to-live policies, automated expiration, and continuous validation that machine identities still serve active purposes.

Strategic implications

The NHI explosion fundamentally changes what identity security means. Organizations must:

1. Treat NHI security as foundational, not supplementary

Machine identity management cannot be an afterthought to workforce IAM. It should be the primary focus given volume ratios.

2. Implement automated discovery and continuous monitoring

Manual discovery projects that catalog machine identities quarterly or annually are obsolete. Discovery must be continuous, automated, and integrated across cloud, on-premises, and SaaS environments.

3. Establish ownership accountability

Every machine identity should have a defined owner (human or system) responsible for its life cycle, access appropriateness, and decommissioning.

4. Deploy time-to-live policies

Default machine identities to expiration rather than persistence. Require active renewal with justification rather than allowing indefinite survival.

5. Budget for NHI management as discrete investment priority

Only 12% have achieved comprehensive, automated life cycle management. The remaining 88% need to invest in tools, processes, and expertise specifically for machine identity governance.

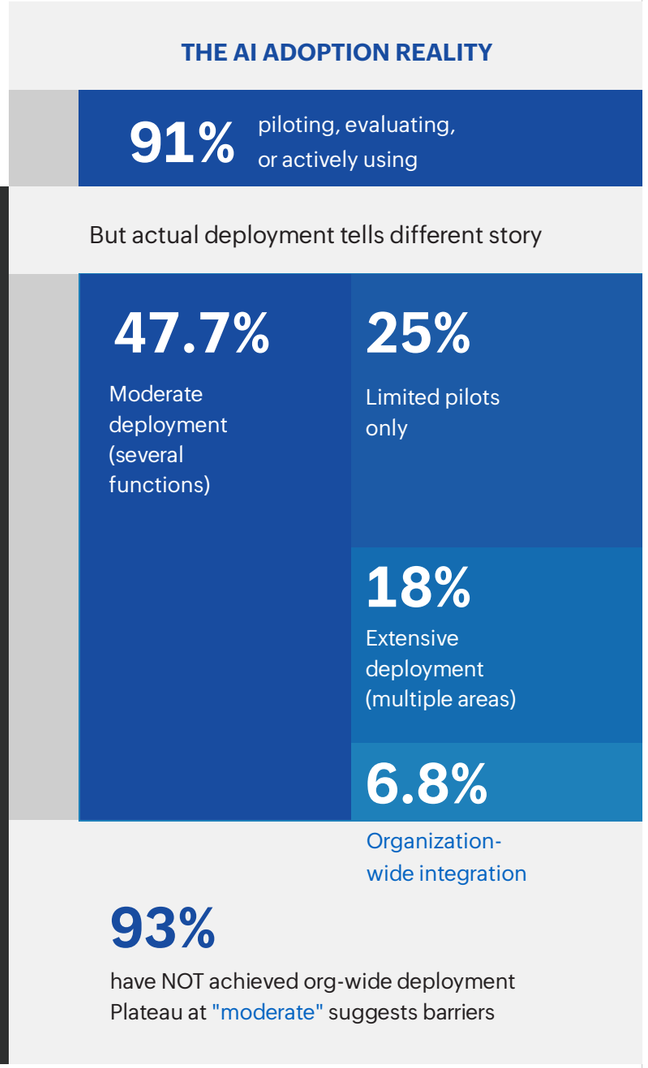
AI adoption in identity security:

More promise than proof

The current state of AI adoption

AI is rapidly entering identity and access management operations, though adoption levels and operational maturity vary dramatically across organizations. The gap between enthusiasm and execution reveals an industry in early experimentation rather than mature deployment.

While 91% of organizations are piloting, evaluating, or actively using AI in IAM operations, only 7% have achieved organization-wide deployment. The moderate deployment majority (47.7%) aligns closely with those reporting mixed experiences, suggesting many remain indefinitely at this plateau if orchestration, integration, and explainability barriers aren't resolved.



The AI paradox:
Opportunities and cautions

Organizations face a dual challenge with AI in identity security, using it for defense while defending against it as a threat vector:

- **AI as a defense**

Organizations leverage AI for improved anomaly detection, automated threat response, predictive analytics, and intelligent policy enforcement. These capabilities promise to extend limited security teams and enhance detection capabilities beyond human cognitive capacity.

- **AI as a threat**

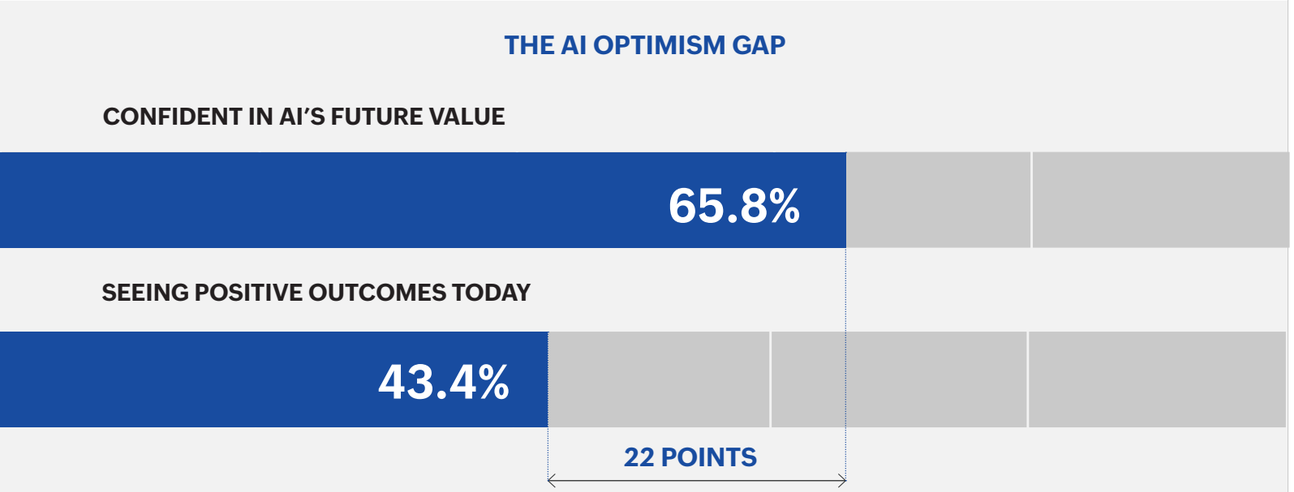
Adversaries deploy AI for sophisticated attacks—deepfakes bypassing biometric authentication, AI-powered social engineering, automated credential stuffing at massive scale, intelligent malware that adapts to defenses. Each defensive AI advancement is matched by corresponding offensive capabilities.

This duality requires parallel investment in both offensive and defensive AI capabilities, further straining already constrained budgets and expertise. Organizations must simultaneously deploy AI to improve their security posture while defending against AI-powered attacks that exploit the same technologies.

The arms race dynamic creates pressure for continuous investment. Organizations that fall behind in AI adoption risk being outpaced both by competitors who use AI more effectively and by adversaries who exploit AI-enabled attack vectors against outdated defenses.

The 22-point optimism gap:
Faith outpacing evidence

While 65.8% express confidence in AI's future value for identity security, only 43.4% currently see positive, expectation-meeting outcomes. This gap suggests that belief is outpacing tangible success—potentially signaling overestimation of AI's near-term readiness in identity operations. Organizations are investing based on anticipated returns rather than demonstrated value.



This gap reveals: Faith-led adoption, not evidence led maturity.

Unrealistic expectations dominate in executive ranks

Many leaders expect AI to deliver near-immediate, transformative value without recognizing the implementation realities. AI requires months of tuning, clean training data, iterative refinement, and organizational change management. The marketing narrative around AI suggests plug-and-play intelligence. The operational reality involves significant configuration, ongoing maintenance, continuous model retraining, and integration complexity. Executives see vendor demonstrations showing polished AI capabilities and extrapolate to their own environments without accounting for data quality issues, integration challenges, or the expertise required for effective deployment.

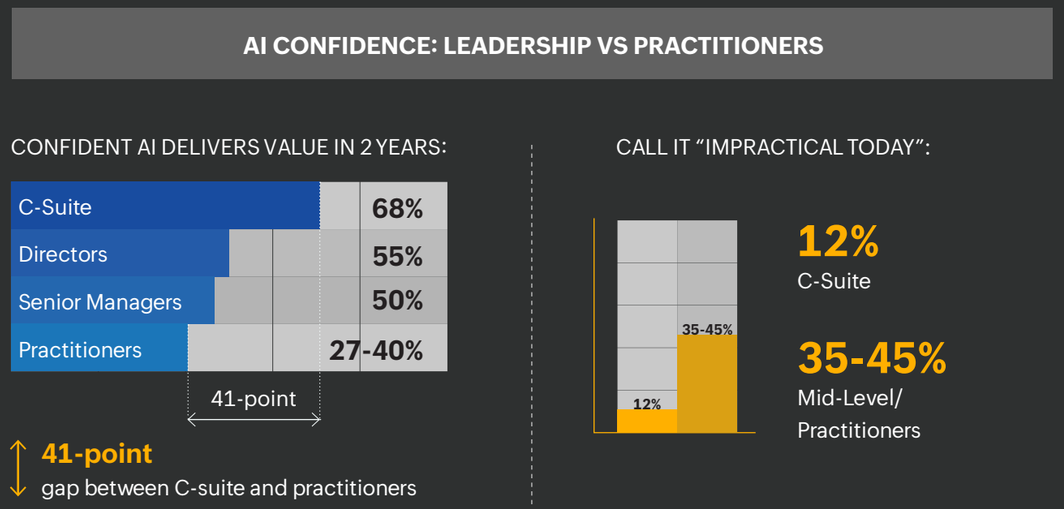
AI is genuinely immature for many IAM use cases

Identity security requires explainability that current AI models struggle to provide comprehensively. When an AI system denies access, flags an account as risky, or recommends privilege removal, security teams need to understand why—not just for operational troubleshooting but for regulatory compliance and audit requirements. Black-box decision-making creates significant challenges. AI is advancing rapidly, but explainable AI for identity contexts remains an evolving discipline rather than a solved problem. Organizations in regulated industries (finance, healthcare, government) face particular challenges when AI recommendations cannot be easily explained or audited.

The perception chasm:
Executives vs. practitioners

The survey reveals a significant divide in AI sentiment between leadership and operational staff:C-suite leaders (68%) are bullish on AI for identity risk modeling and analytics; only 27% of mid-managers agree it's practical today.

This disconnect raises a critical question: Is this visionary leadership or executive detachment from operational reality?



Competitive and board pressure is an important factor. Fear of falling behind drives investment decisions even without clear ROI evidence. Boards ask “What’s our AI strategy?” creating pressure to demonstrate AI adoption regardless of readiness. No executive wants to report “We’re not doing AI” when competitors claim (often exaggeratedly) to be AI-first. This creates incentives to champion AI initiatives even when internal feedback suggests caution. In addition, executives are inherently wired to think in three to five year strategic horizons.

From that perspective, current implementation challenges are temporary hurdles on the path to transformation. Practitioners operate on quarterly or monthly timelines where current challenges directly impact their ability to deliver results. This temporal misalignment creates perception gaps where executives see “We’re making progress toward a transformative goal,” while practitioners see “This isn’t working today and we don’t know when it will.”

So, who’s right here? Both perspectives are valid, but practitioners’ skepticism is likely more grounded in current reality. Executives are correct that AI will eventually deliver significant value in identity security. Practitioners are correct that eventually is not now and the path from here to there is longer and harder than executive timelines suggest. The danger lies in the execution pressure this creates: executives set aggressive AI deployment timelines based on optimistic assumptions, forcing practitioners to deploy immature capabilities that don’t deliver expected results, eroding credibility for future AI initiatives.

What’s holding AI back?

Trust, talent, or tangible ROI?

All three factors constrain AI adoption in identity security, but their relative importance varies by organizational context:

1 Trust limitations stem from explainability gaps

Organizations struggle to trust AI systems that cannot explain their recommendations in ways humans can validate. When an AI system recommends revoking access for a user, security teams need to understand whether that recommendation stems from legitimate risk indicators or spurious correlations in training data. When AI flags an authentication attempt as anomalous, incident responders need to know which behavioral factors triggered the alert. Without this explainability, organizations cannot distinguish between AI insights they should act on and AI errors they should ignore. The trust gap is particularly acute in regulated industries where “the AI said so” doesn’t satisfy audit requirements or legal standards.

2 Talent shortages create a catch-22

Implementing and maintaining effective AI systems requires expertise that organizations already struggling with IAM talent shortages don’t possess. AI in identity security requires professionals who understand both identity operations and data science, machine learning, model governance, and AI security. This hybrid expertise is rare and expensive. Organizations face a paradox: they need AI to extend limited team capabilities, but implementing AI effectively requires specialized capabilities they lack. Many attempt to bridge this gap through vendor-provided AI (which limits customization and creates dependency) or through consultants (which doesn’t build internal capability).

3 Tangible ROI remains elusive for most

Organizations struggle to demonstrate clear returns on AI investments in identity security. Success metrics are often unclear: is AI successful if it reduces false positives by 30%? If it saves analysts 10 hours per week? If it detects 5% more anomalies? Without clear baseline measurements and agreed success criteria, organizations cannot definitively prove AI delivers value. The moderate deployment plateau (47.7%) likely reflects organizations that deployed AI to several functions, saw modest improvements insufficient to justify broader expansion, and stalled waiting for clearer ROI evidence before investing further.

Is AI a viable substitute for the talent shortage?

This raises ethical and practical concerns:

The trade-off question

How do organizations justify replacing human expertise with AI when AI implementation itself requires significant capital investment, training data preparation, and ongoing security and compliance oversight?

Institutional memory

When human experts leave and AI systems make identity decisions, who retains the contextual knowledge that informed those decisions? AI can automate routine tasks but cannot replicate years of accumulated judgment about organizational culture, risk tolerance, and exception handling.

Regulatory uncertainty

With limited regulations on AI use in security operations, organizations outsourcing identity decisions to AI face uncertain legal exposure if those decisions result in breaches or compliance failures.

One in five organizations in the US and Canada cite IAM skill shortages and complexity as major challenges. These regions show increased reliance on AI augmentation as a way to bridge the expertise gap rather than restructuring tool sets.

Is it ethical to outsource critical identity decisions to AI when internal expertise is eroding?

This cuts to fundamental questions about organizational knowledge and accountability. When human experts make identity decisions, they accumulate contextual understanding about why certain policies exist, how exceptions should be handled, what organizational risk tolerance looks like, and how business processes intersect with access requirements.

When AI systems automate these decisions without building human understanding, institutional memory erodes. Ten years from now, when the AI system needs refinement or replacement, organizations may lack personnel who understand the identity security domain deeply enough to guide that evolution. The ethical concern isn't AI use itself; it's the erosion of institutional memory and the creation of dependencies on systems no one fully understands.

AI as augmentation, not replacement

The data suggests AI will serve primarily as an augmentation layer rather than a wholesale replacement for human talent, at least in the near term. Organizations that treat AI to extend existing expertise will likely see better outcomes than those attempting to substitute AI for missing skills.

The pattern reveals organizations starting with high-value, measurable use cases before tackling complex analytical functions. This pragmatic approach, piloting AI where it demonstrably improves outcomes before expanding the scope, appears more sustainable than ambitious organization-wide deployments.

If organizations deploy AI to extend the capabilities of existing teams, enabling them to accomplish more without burning out, that represents fair utilization of technology to address workforce constraints. If organizations deploy AI as justification for not investing in training, not hiring sufficient staff, or not addressing root causes of talent scarcity (inadequate compensation, poor working conditions, lack of career development), that's cost-shifting disguised as innovation. The fairness question hinges on whether AI augments human capability or provides cover for underinvestment in people.

AI USE CASES INTEREST GRAPH

Use case	Respondents	Interest level
Automated provisioning/ deprovisioning *Clear ROI, measurable results*	42%	MODERATE
Behavioral analytics/ anomaly detection *High value but requires data maturity*	38%	HIGH
Risk-based adaptive authentication *Direct security improvement*	35%	HIGH
Policy recommendation engines *Complex but addresses governance gaps*	27%	HIGH
Threat detection and response *Integration challenges limit adoption*	23%	MODERATE

Legal landscape remains uncertain:

No comprehensive regulatory framework governs AI use in identity and access management. When AI systems make erroneous decisions resulting in inappropriate access, data breaches, or compliance violations, liability questions remain unresolved:

- → Is the organization liable for decisions made by AI systems it deployed but doesn't fully understand?
- → Are vendors liable for AI models that produce harmful outcomes when applied in contexts they didn't anticipate?
- → How do regulatory frameworks designed around human decision-making apply when AI makes access determinations?
- → Can organizations demonstrate reasonable care in access governance if they cannot explain how their AI systems reached specific conclusions?

These questions will be tested through litigation and regulatory proceedings over the coming years, creating legal uncertainty for organizations pursuing aggressive AI adoption.

Are leaders overlooking the training data challenge (cost, compliance, and security)?

Effective AI requires vast quantities of properly structured, labeled, and representative data. Most identity data exists fragmented across multiple systems with inconsistent formatting. Consolidating, cleaning, and labeling this data for AI training requires substantial effort—often 6–12 months of work before AI deployment can begin. The labor costs for data preparation frequently exceed AI platform licensing costs, yet organizations rarely budget adequately for this invisible but essential work. Leaders see AI platform costs but miss the far larger data preparation investment required for success.

Additionally, training identity security AI models requires access to sensitive data: authentication logs, access patterns, user behavior, and privileged account activity. Using

production data for AI training raises privacy concerns under the GDPR, the CCPA, and similar frameworks, with murky compliance implications across jurisdictions.

Centralizing identity data for AI training also creates security risks; a compromised training environment could expose comprehensive information about organizational access patterns, privilege structures, and security controls. Organizations must secure not just production systems but also AI development and training environments, effectively doubling the attack surface while navigating unresolved compliance questions.

Will AI replace human talent in identity security?

The survey data strongly suggests no, at least not in the foreseeable future. Several factors point toward augmentation rather than replacement:

Trust gap limits autonomous operation

Only 43% see AI delivering positive outcomes today, creating hesitation about expanding AI decision-making authority. Organizations won't fully automate consequential access decisions without proven reliability.

Complex context requires human judgment

Identity decisions often require organizational context, understanding of business priorities, political considerations, and exception handling that AI cannot replicate from data patterns. Access decisions involve nuances existing in human institutional memory, not training datasets.

Accountability requirements assume human decision-makers

Regulatory and legal frameworks still expect humans to be accountable for access governance outcomes. While this will evolve, current environments requires humans in decision chains for consequential determinations.

Implementation expertise AI systems require

AI doesn't implement, train, tune, or govern itself. Organizations need human expertise to deploy AI effectively, maintain it operationally, and refine it as context changes.

Why humans run AI rather than AI-run operations

Context and judgment requirements

Identity security decisions require understanding organizational context, political considerations, business priorities, and risk tolerance that AI cannot replicate from data patterns alone. Access decisions involve nuances: This person needs access even though they're not in the standard role because they're covering for someone on leave; this department always requests broad access but we know they only use 20% of it; this system is being decommissioned next month so we shouldn't grant long-term access. AI trained on data patterns cannot capture this contextual knowledge that exists in human institutional memory.

Accountability and liability

Legal and regulatory frameworks assume human decision-makers for consequential access decisions. While this will evolve, the current regulatory environment requires humans to be accountable for access governance outcomes. Organizations cannot deflect responsibility to AI systems in ways regulators will accept.

Edge case handling

AI excels at handling the 80-90% of routine, pattern-matching decisions. Identity security also involves 10-20% of edge cases, novel situations, and exceptions that fall outside training parameters. Human expertise becomes critical precisely when established patterns don't apply. Organizations need human judgment available when AI encounters situations it cannot handle.

The future division of labor

AI will handle volume (processing thousands of access requests, analyzing millions of authentication events, monitoring continuous user behavior across sprawling environments) while humans handle complexity (evaluating access requests for sensitive systems, investigating anomalous behavior flagged by AI, making risk-based decisions about policy exceptions, and governing AI systems themselves). This plays to respective strengths: AI provides speed, consistency, and pattern recognition at scale; humans provide judgment, contextual understanding, and accountability.

Organizations should prepare for this hybrid model by developing new skills within identity teams: understanding how to govern AI systems, interpreting AI recommendations critically, refining models based on operational outcomes, and maintaining oversight without becoming bottlenecks. This requires different capabilities than traditional IAM roles but doesn't eliminate the need for human expertise—it transforms what expertise means.

The defining force of 2026

With over 42% of organizations citing talent scarcity as a major 2026 challenge, and IAM specialists increasingly difficult to find and retain, consolidation has transformed from a cost optimization exercise into a survival strategy. Organizations cannot hire enough platform specialists to manage fragmented stacks while simultaneously governing 100:1 machine-to-human identity ratios. Architectural simplification isn't a nice-to-have efficiency gain; it's an operational necessity.

The most defining force shaping identity security in North America isn't AI; it's the shortage of skilled practitioners needed to manage increasingly complex identity ecosystems.

This talent constraint explains why consolidation momentum persists despite legitimate concerns about vendor lock-in, migration complexity, and capability trade-offs.

Organizations recognize they must choose between:

- → Simplified architectures their limited teams can actually manage effectively.
- → Complex fragmented environments that exceed their team's capacity, creating security gaps and operational failures.

When framed this way, the consolidation decision becomes obvious despite its challenges.

Verdict: Is AI a C-suite buzzword (or not)?

- **It's a buzzword because**

  Board members read about AI transforming business. Analysts publish reports about AI-driven security. Competitors announce AI initiatives. This creates pressure for executives to demonstrate AI adoption regardless of readiness or ROI. AI strategy becomes a checkbox item in board presentations, creating incentives to pursue AI for appearance rather than substance.

- **It's not just a buzzword because**

  Genuine strategic potential exists. The machine identity explosion, talent shortages, and scale of modern identity environments create real need for capabilities that only AI can provide. Executives recognize (correctly) that manual identity governance cannot scale to 100:1 machine-to-human ratios. The buzzword status doesn't negate the legitimate strategic imperative—it just creates risk that organizations pursue AI prematurely or inappropriately.

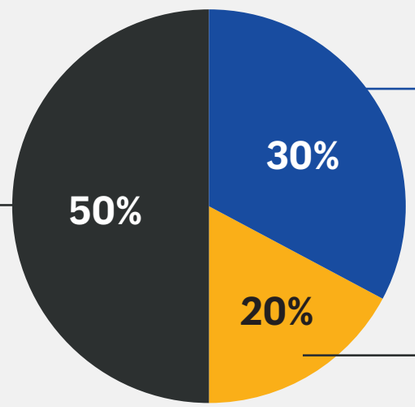
The identity stacks of today:

Fragmented by design, not by accident

The multi-vendor reality

Modern identity security involves multiple specialized tools such as IAM, PAM, MFA, SSO, IGA, UEBA, and CIEM, creating a vendor landscape that most organizations find challenging to navigate.

VENDOR SPRAWL ACROSS ORGS



2-4 VENDORS

50%

Best-of-breed by design

1 VENDOR (CONSOLIDATED)

30%

Deliberate platform choice or small scale

5+ VENDORS

50%

M&A complexity or dept. autonomy

70%
juggle multiple IAM tools

Nearly
3 in 4
face multi-vendor complexity

Nearly three in four organizations juggle multiple IAM tools. Tool fragmentation scales with organization size; over half of large enterprises manage three or more IAM vendors, while smaller firms manage around one or two.

Is tool sprawl maturity or architectural indecision?

The data reveals a complexity tipping point: operational friction begins as soon as an organization crosses two identity tools. Licensing, policy harmonization, and skill overhead multiply exponentially rather than linearly.

Organizations with multiple specialized tools recognized that identity security encompasses distinct problem domains requiring different capabilities. Privileged access management differs fundamentally from workforce identity governance, which differs from consumer authentication, which differs from cloud entitlement management. Organizations that selected specialized tools for each domain demonstrated sophisticated understanding of these distinctions. In this view, tool diversity reflects maturity, recognizing that one-size-fits-all platforms sacrifice depth for breadth.

The same organizations failed to establish principles for how tools would interoperate, failed to assess cumulative complexity before adding each new tool, and failed to recognize that specialization has diminishing returns once integration overhead exceeds functional benefits. Mature organizations would have asked before tool five: "At what point does adding another tool create more problems than it solves?" Most didn't ask this question, instead accumulating tools until operational burden forced reconsideration. In this view, tool sprawl reflects architectural indecision—prioritizing tactical capability additions without strategic integration planning.

However, the truth lies in synthesis. Tool sprawl often begins as mature recognition of distinct requirements but becomes architectural indecision when organizations lose sight of integration costs. The initial tools make sense. Somewhere between tools three and six, the architecture crosses a threshold where complexity overwhelms capability, but organizations lack clear governance to recognize or act on this transition.

Tool sprawl exists partly because organizations lack expertise to consolidate. Selecting, implementing, and migrating to unified platforms requires deep identity security expertise, platform-specific knowledge, and project management capability. Organizations lacking these skills default to accumulating tools rather than replacing them.

Simultaneously, tool sprawl creates and perpetuates skill gaps. Managing multiple platforms requires spreading expertise thin across many technologies, developing shallow knowledge of many tools rather than deep expertise in any. Training budgets get consumed teaching basic competency across vendors. New hires face steeper learning curves. Turnover increases as skilled practitioners seek less chaotic environments.

The bigger picture:
Why fragmentation persists

Enterprises continue operating with fragmented stacks despite known inefficiencies for several reasons:

Best-of-breed philosophy

Organizations historically adopted specialized tools for specific functions, one vendor for MFA, another for PAM, a third for IGA, believing this approach delivered superior capability in each domain.

Merger and acquisition activity

Growth through merger and acquisition inherits disparate identity systems, each with existing contracts, integrations, and institutional knowledge.

Departmental autonomy

Different business units often select their own tools independently, creating organic sprawl without centralized oversight.

Fear of disruption

Migration risk feels higher than the ongoing cost of complexity. Organizations know consolidation would help but fear operational disruption during transition.

Contract obligations

Multi-year vendor agreements create financial barriers to change. Consolidation might require breaking contracts, paying termination fees, or waiting for renewal cycles. These financial constraints can force organizations to maintain fragmented architectures longer than operationally optimal.

MULTI-VENDOR OPERATIONAL PAIN POINTS

HIGHER TOTAL COST OWNERSHIP

40.7%

Licensing + maintenance + overhead

SKILL GAPS ACROSS PLATFORMS

37.4%

Cannot hire/train for all tools

INTEGRATION COMPLEXITY

34%

Each connection = maintenance burden

INCONSISTENT USER EXPERIENCE

30%

Different workflows per tool

DATA SILOS PREVENTING VISIBILITY

28%

Cannot correlate across systems

- 99.44% face tangible friction
- Top 3 challenges all stem from multiplicity

The time tax of vendor sprawl

This administrative overhead represents millions in lost productivity annually. When senior identity security professionals spend 35% of their time coordinating vendors, managing license renewals, troubleshooting integration failures, and reconciling policy differences across platforms, they cannot pursue proactive security improvements, threat hunting, or strategic initiatives. The opportunity cost of vendor sprawl extends far beyond licensing fees.

***One in three organizations spend more time managing IAM vendors than managing privileged users.** Nearly 40% say managing multiple IAM vendors consumes excessive time compared to ~20% in smaller firms with single-vendor setups.*

The complexity paradox

Even organizations with only 2–4 vendors report operational pain mirroring those with 5–6. Once an organization introduces more than two identity systems, the overhead in licensing, policy harmonization, and administrative skill depth multiplies exponentially.

Complexity doesn't scale gradually, it spikes early.

Each tool added creates more integration burden than the previous one. Beyond integration count, each additional tool introduces policy synchronization challenges, workflow coordination requirements, user experience inconsistencies, and administrator expertise needs. The cognitive load multiplies faster than tool count.

At what point does adding one more tool become catastrophic?

The data suggests this tipping point occurs between two and three vendors for most organizations:

- Organizations managing two vendors report elevated integration challenges but generally maintain operational control.
- Organizations managing three vendors report that integration overhead begins consuming resources intended for security improvements.
- Organizations managing four or more vendors frequently report that identity teams spend more time maintaining architecture than operating it.

The catastrophic threshold varies by organizational capability. Organizations with strong integration expertise, robust automation practices, and adequate staffing might sustain four or five vendors. Organizations with limited resources, manual processes, and high staff turnover might find two vendors overwhelming.

The universal principle: every organization has a complexity threshold. Adding tools beyond this ceiling doesn't increase capability; it degrades it by overwhelming teams' ability to operate coherently. Organizations should identify their ceiling and architect accordingly rather than assuming more tools always means more capability.

What would true identity maturity look like if consolidation wasn't the benchmark?

Organizations achieving genuine maturity demonstrate:

Comprehensive visibility across all identity types with minimal manual effort

Can security teams answer within minutes which identities (human and machine) have access to specific sensitive resources across all environments? This requires unified data models and consistent policy frameworks that fragmented tools struggle to provide.

Automated life cycle management at scale

Are identity privileges tightly coupled to business context through automated provisioning and deprovisioning? Do machine identities have enforced expiration? Can the organization onboard 1,000 new employees or deploy 10,000 new containers without manual identity administration? Scale demands automation that fragmented architectures make difficult.

Security teams focused on threat response rather than vendor coordination

What percentage of identity team time goes to strategic security work versus administrative overhead? Mature organizations maximize security work; immature ones drown in administrative tasks.

Clear, auditable governance regardless of underlying architecture

Can the organization demonstrate continuous compliance through automated evidence collection rather than periodic manual audits? Can it produce audit trails showing who approved access, when, and why? Governance maturity requires integrated workflow and reporting that fragmented tool environments cannot deliver.

Resilience to partial system outages

Can identity operations continue during partial system failures without critical capabilities going offline? Fragmented architectures where capabilities depend on integration chains create brittleness; consolidated or well-orchestrated architectures maintain resilience.

By these outcome measures, consolidation often correlates with maturity because unified platforms make it easier to achieve these capabilities. But the goal is these outcomes, not consolidation for its own sake.

Indicators of true identity maturity

Indicator	Traditional view	Emerging view
Number of tools	More = more capable	Fewer = more efficient
Integration points	Many = comprehensive	Fewer = less risk
Team-time allocation	Management overhead acceptable	Strategic work should dominate
Machine identity visibility	Nice to have	Non-negotiable foundation

Consolidation:

4

From debate to execution

The consolidation consensus

The survey reveals overwhelming support for vendor consolidation, suggesting it has moved from controversial idea to strategic consensus.

However, execution lags intent

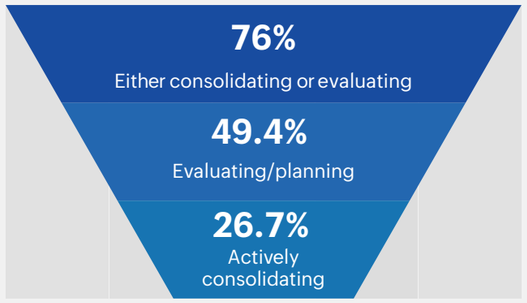
Organizations that have progressed into active consolidation exhibit several consistent enabling factors. Executive sponsorship with clear decision authority ensures that conflicts, resource needs, and trade-offs are resolved without delay. Realistic timelines, often 18 to 36 months, acknowledge the scope and interdependencies inherent in identity consolidation. Successful programs also rely on phased execution that protects operational stability while delivering incremental value in high impact areas. These organizations invest in adequate resourcing, including external expertise and temporary capacity, to prevent migration activities from overwhelming existing teams. They also define success through multidimensional metrics that include security posture, operational efficiency, and team experience in addition to cost outcomes.

In contrast, the majority still in planning or assessment face structural barriers that limit progress. Budget constraints reduce access to migration tooling, consulting support, and supplemental staffing. Persistent competing priorities push consolidation behind other initiatives, while broader organizational change capacity is already taxed by parallel transformations. Leadership often demonstrates caution toward transitional risk, slowing decision making. Contractual obligations also influence timing, either imposing financial penalties for early termination or forcing organizations to wait for renewal cycles.

73%

express support for consolidation (32% strong + 41% moderate). Only 10% are skeptical or opposed. Just 0.28% report having no plans for vendor consolidation. Statistically, resistance has vanished. The conversation has definitively shifted from "Should we consolidate?" to "How quickly can we consolidate?"

FROM INTENT TO ACTION:
THE EXECUTION GAP



BARRIERS:

- Migration complexity
- Budget cycles and competing priorities
- Resource constraints during transition
- Contractual obligations

Who's driving consolidation?

The survey reveals a notable split in how different roles perceive consolidation:

- **Leadership's view**

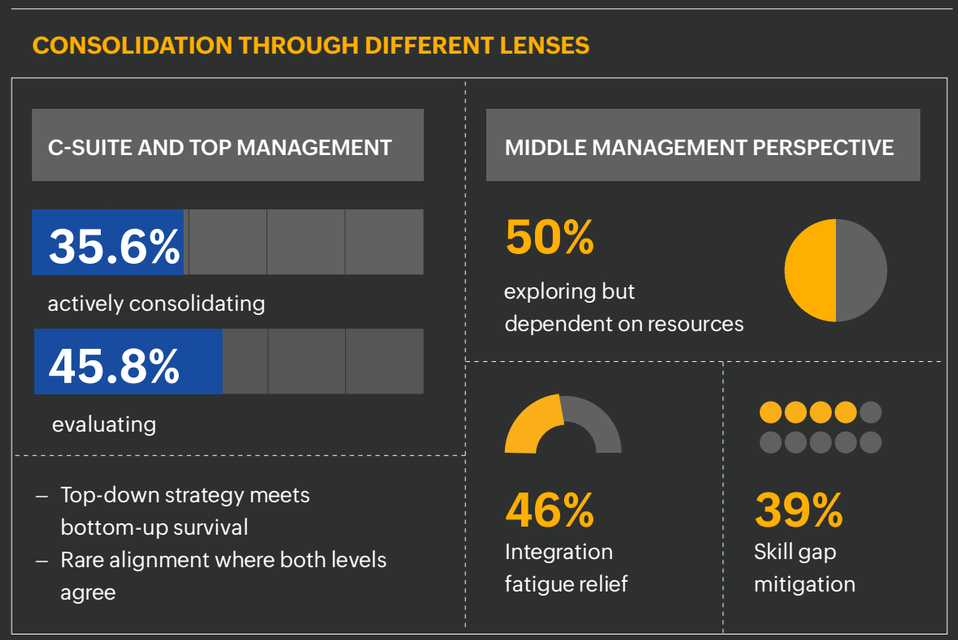
  The C-suite frames unification around cost efficiency and governance predictability. With 35.6% actively consolidating and another 45.8% evaluating consolidation, nearly the entire leadership tier is steering organizations toward fewer, unified identity platforms.

- **Management's view**

  Middle managers emerge as the most evaluation-heavy cohort, with 50% exploring consolidation but viewing it as relief from process fatigue rather than strategy—a way to get more done with less chaos.

When executives pursue consolidation purely for cost savings without considering operational impact, implementations fail because teams lack incentive to make them work. When operational teams pursue consolidation for relief without demonstrating financial value, they fail to secure executive sponsorship and resources.

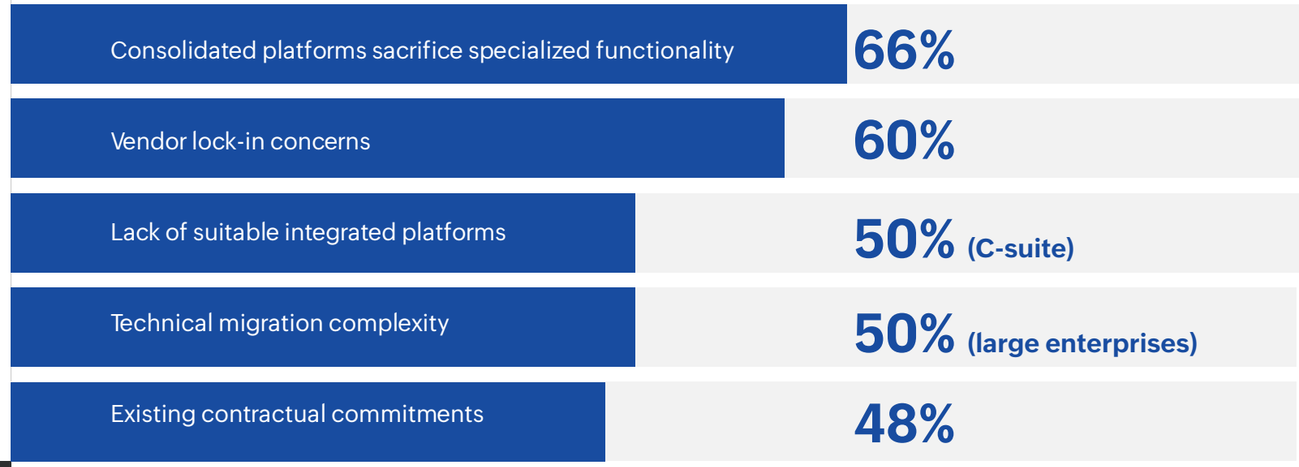
Organizations progressing from evaluation to active transition are those where executives and managers share consolidation rationale. Leadership communicates cost efficiency and governance as strategic drivers while acknowledging operational burden and committing resources to ease transition. Teams embrace consolidation as a path to relief while demonstrating ROI through reduced vendor management time and improved security outcomes.



Resistance patterns:
Why the 10% remain skeptical

Among those skeptical of consolidation, the objections are practical rather than philosophical:

Top reasons for consolidation skepticism



These are often surmountable barriers rather than fundamental blockers. Contracts expire. Modern platforms increasingly offer specialized capabilities. The best-of-breed myth that integrated platforms are inherently inferior is declining as consolidated solutions mature.

Regional patterns

Factor	United States	Canada
Consolidation active/ evaluating	**76%**	**80%**
Primary barrier	Skill gaps, technical migration risk	Contracts, governance structures
Budget approach	Higher dynamism (growth and optimization)	Consolidation-led compression

Sectoral blockers

Industry	Primary consolidation barrier
Architecture/ engineering	Technical complexity (50%)
Finance	Lack of suitable platforms (37.5%), regulatory concerns
Healthcare	Organizational resistance (31%), governance-heavy environments
Legal	Lack of integrated platforms (33%), risk-averse

The finance and healthcare sectors face the highest consolidation barriers, largely due to regulatory complexity and compliance requirements that create legitimate hesitation about platform changes.

The lock-in fear:
Trading one form of constraint for another

C-suite leaders (66%) are far more likely than senior managers (48%) to cite vendor lock-in risks as the biggest barrier to consolidation. This reflects executive concern about long-term strategic flexibility. Yet the same survey shows organizations already experiencing lock-in effects from fragmented stacks, integration dependencies, skill investments, and contractual commitments that make any change difficult. The question becomes: which form of constraint is preferable?

Legitimate lock-in concerns include:

C-suite leaders (66%) are far more likely than senior managers (48%) to cite vendor lock-in risks as the biggest barrier to consolidation. This reflects executive concern about long-term strategic flexibility and negotiating leverage. Yet the survey data reveals organizations already experiencing lock-in effects from fragmented stacks:

- **Integration dependencies**

When multiple systems integrate with each other and with dozens of applications, replacing any single component requires rewiring numerous connections, creating lock-in to the entire architecture.

- **Skill investments**

Teams develop expertise in specific platforms through training, certification, and experience. These sunk investments in human capital create resistance to changing platforms even when alternatives might be superior.

- **Contractual commitments**

Multi-year agreements, committed spending, and enterprise licensing create financial lock-in regardless of whether organizations use one vendor or many.

- **Data gravity**

Identity data, access policies, audit logs, and governance workflows embedded in existing systems create migration barriers. Moving this data between systems requires significant effort regardless of platform architecture.

The question becomes: which form of constraint is preferable? Lock-in to a single comprehensive platform with unified data, consistent interfaces, and simplified operations, or lock-in to a fragmented architecture with integration dependencies, coordination overhead, and multiplied complexity?

Consolidation strategy:
Gradual vs. comprehensive

The majority favor gradual migration (38%) rather than “rip and replace,” reflecting the need to minimize disruption while achieving consolidation benefits over time. The hybrid model (32%), consolidating where possible while retaining specialized tools where necessary, represents a pragmatic middle ground, acknowledging that consolidating everything may not be optimal for all organizations.

The gradual migration majority reflects organizational wisdom that consolidation must preserve stability while achieving benefits over time, whereas the hybrid model represents pragmatic recognition that consolidating everything may not be optimal; some specialized tools might warrant retention where they deliver irreplaceable value.

PHASED CONSOLIDATION APPROACH (24 MONTHS)

Gradual migration to unified platform

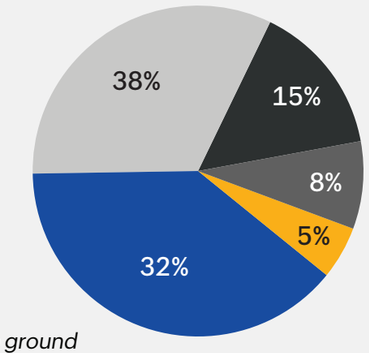
38%

Minimize disruption, deliver incremental value

Consolidate select tools, keep best-of-breed

32%

Hybrid model, pragmatic middle ground



Wait for current contracts to expire

15%

Financial constraints drive timing

Actively evaluating platforms

8%

Earlier stage, vendor selection in progress

No consolidation planned

5%

70%

favor gradual or hybrid approaches

→ Reflects need to balance improvement with risk

This challenges how organizations use efficiency gains. The ethical imperative: maintain sufficient capability to operate consolidated platforms effectively and provide oversight. The ethical breach occurs when organizations use consolidation primarily as a headcount reduction strategy rather than capability enhancement. When underwater teams remain underwater after consolidation because staffing wasn’t maintained, consolidation has failed ethically and practically.

With 92% keeping budgets stable or growing, is it ethical to redirect savings from consolidation into other strategic areas rather than reinvesting in people and oversight?

Identity security investments:

Recalibrations and priorities for 2026

Budget outlook:

Stability with strategic reallocation

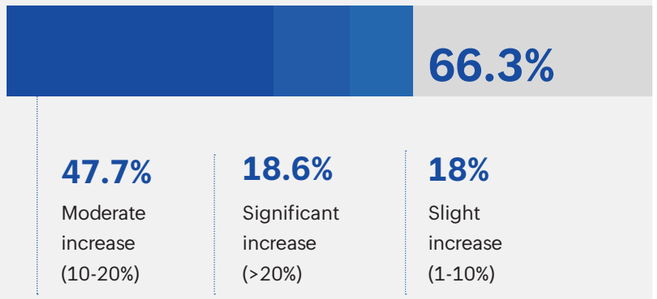
The survey paints an optimistic picture of identity security investment for 2026. Over 92% of respondents expect budgets to grow or remain constant. Identity security remains a strategic investment area, not a cost center to be minimized.

Understanding budget cuts

Among the minority expecting decreases, the reasons reveal strategic optimization rather than retreat.

Nearly 60% of expected budget cuts are efficiency-driven, not reductions in capability or scope. ***This finding reframes the consolidation conversation: it's not a budget cut; it's a reallocation strategy.***

2026 BUDGET EXPECTATIONS



- 92.6% expect growth or stability
- Identity security remains a strategic investment
- "Cuts" often mask strategic optimization

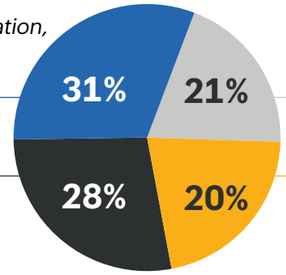
Organizations typically achieve 40–50% reduction in total identity operations cost within three years while simultaneously improving security outcomes. However, they experience a J-curve where costs rise initially (migration, training, consulting, parallel operations) before dropping significantly as consolidation delivers efficiency gains.

Consolidation delivers measurable financial and operational returns that go beyond simple budget reshuffling. In the near term, organizations reduce redundant licensing, streamline vendor management, and cut professional services duplication. These steps typically remove a significant portion of IAM or PAM spend while also reducing procurement and administrative overhead. Operational efficiency improves as teams maintain fewer integrations, troubleshoot issues more quickly through unified visibility, and simplify upgrades without multi-vendor coordination. Administrators work within a single ecosystem, which reduces context switching and frees substantial time for higher-value work.

THE REAL STORY BEHIND PERCEIVED BUDGET CUTS

31%
Consolidation reducing licensing/ operational costs
Strategic optimization, not capability cut

21%
Moving to in-house tools
Build vs. buy rebalancing



28%
Shifting to more cost-effective solutions
Platform rationalization

20%
Overall cost optimization/ budget cuts
Only 1 in 5 cite actual budget pressure

- 60% of "cuts" = efficiency-driven reallocation
- Organizations spending smarter, not less

Longer term, consolidation enables strategic gains that compound the initial savings. Unified platforms accelerate the rollout of new capabilities, enhance security through consistent policies and centralized detection, and strengthen compliance by eliminating gaps created by fragmented tooling. Teams can shift focus from maintenance to innovation, improving overall security maturity. Talent-related benefits add further ongoing returns. Training becomes simpler, onboarding gets quicker, retention improves, and hiring can target deeper expertise rather than broad tool coverage.

United States

Shows higher budget dynamism, balancing aggressive investment increases (71% expect growth) against selective cost recalibration (only 6.8% expect decreases). This reflects larger average organization sizes, more diverse vendor landscapes requiring rationalization, and cultural comfort with significant investment swings.

Canada

Demonstrates more pronounced movement toward budget compression driven by unification efforts. Two-thirds (66.67%) of Canadian respondents experiencing decreases link them directly to consolidation reducing licensing and operational costs. This suggests Canadian organizations may be further along in consolidation journeys, already realizing cost benefits American organizations are still pursuing.

The pattern: the US identity security market is entering hybrid maturity (growing scope, refining allocation); Canada is entering a stabilization stage (prioritizing simplification and efficiency over expansion).

Investment priorities for 2026

This distribution reveals dual-track maturity emerging: practitioners prioritizing integration and automation (addressing today's pain), leaders emphasizing convergence and governance (building tomorrow's architecture). Both paths ultimately converge on the same goal: identity unification.

The sequencing matters. Organizations invest heavily in integration and AI first, attempting to manage fragmentation through orchestration and automation before committing to consolidation. This reflects caution about consolidation risk and desire to improve the current state before major architectural change. However, this sequence may extend timelines for achieving simplification because integration investments can perpetuate fragmented architecture rather than replacing it.

TOP IDENTITY SECURITY PRIORITIES FOR 2026

AI-POWERED ANALYTICS

43%

Despite maturity concerns, investment surges

INTEGRATION AND INTEROPERABILITY

41-42%

Addressing fragmentation pain directly

ZERO TRUST ARCHITECTURE

40%

Foundational security model evolution

SECURING NON-HUMAN/AI IDENTITIES

36%

Recognition of NHI challenge finally emerging

PRIVILEGED ACCESS MANAGEMENT

35%

Core capability modernization

VENDOR CONSOLIDATION

21-24%

Lower rank but universal interest

- → Practitioners chase integration and automation
- → Leaders prioritize convergence & governance
- → Both paths converge on identity unification

Alignment between challenges and investments

For perhaps the first time, identity challenges and investments are finally aligned. The same pain points driving identity fatigue—governance gaps (49%), compliance pressure (48%), managing emerging identity complexities (46%)—are now the top investment priorities.

CHALLENGES DRIVING INVESTMENT PRIORITIES

TOP CHALLENGES	CORRESPONDING INVESTMENTS
Securing basics (governance hygiene) **49.15%**	Integration for governance visibility **42%**
Compliance and market demands **47.57%**	AI for automation at scale **43%**
Managing modern identity complexity **46.02%**	Zero Trust for modern architecture **40%**
Recruiting/retaining skilled staff **41.94%**	Recruiting/retaining skilled staff **24%**

⚠ BUT: <25% have dedicated budgets or expertise to execute these priorities

→ Strategically aligned but operationally underprepared

However, fewer than one in four organizations report having dedicated budgets or sufficient internal expertise to execute on these priorities. This reveals a market that's strategically aligned but operationally underprepared. Organizations know what they need to do; they lack resources or capabilities to execute effectively.

This gap suggests budget growth alone won't suffice if not coupled with capability building. Organizations adding budget without adding expertise will struggle to deploy resources effectively. The limiting factor isn't money; it's skilled people who can execute transformation.

Skills shortage as an investment driver

The talent scarcity challenge (42%) may be the most significant factor shaping 2026 investments. With skilled IAM professionals increasingly difficult to find and retain, organizations are forced toward:

1. **Consolidation** to reduce the number of platforms requiring specialized expertise.
2. **AI augmentation** to extend existing team capabilities.
3. **Automation** to eliminate manual processes that consume skilled resources.

This creates a self-reinforcing cycle: talent shortages push organizations toward consolidation and AI, which in turn reduce demand for specialized multi-platform skills while increasing need for different expertise in platform management and AI governance.

Parting thoughts:

The 2026 Identity Security Outlook

The survey reveals identity programs splitting into two strategic camps that may ultimately converge:

Platform consolidators

Organizations seeking operational efficiency through vendor reduction, unified governance, and architectural simplification. They prioritize eliminating the integration tax, reducing vendor management overhead, and building coherent identity infrastructure as foundation.

Modernizers

Organizations layering AI capabilities, enhanced automation, and machine identity management atop existing systems without full structural consolidation. They prioritize maintaining current operations while adding capabilities, avoiding migration risk, and evolving gradually.

These aren't mutually exclusive paths. The market's next equilibrium will likely be hybrid, AI-driven orchestration unifying a rationalized (not necessarily single) identity fabric. Organizations will consolidate to reduce self-inflicted complexity while using AI and automation to manage remaining complexity efficiently.

What security leaders are thinking about the trajectory of identity security

As cybersecurity leaders plan for 2026, several themes emerge that shape strategic thinking and investment priorities:

Consolidation has moved from aspiration to execution planning

Consolidation is no longer a debate. With broad support and almost no organizations opting out, the focus has shifted to execution. Leaders now concentrate on sequencing, resourcing, and limiting disruption as fragmented stacks are widely seen as creating unacceptable operational strain. The overwhelming share of organizations already consolidating or actively evaluating consolidation reflects a market consensus that complexity has outgrown the capacity of current teams and tools.

This momentum is driven by day-to-day pain rather than vendor influence. Teams spend more time managing vendors than managing security, costs are rising, skills are stretched, and fragmented visibility weakens threat detection. These pressures created bottom-up urgency that aligned with leadership-level cost concerns. The result is a stronger and more durable consolidation push than earlier cycles motivated mainly by budget reduction.

AI adoption is proceeding despite operational uncertainty

The 22-point optimism gap between future expectations (65.8% confident) and current outcomes (43.4% seeing positive results) doesn't appear to slow investment. Organizations bet on AI's potential rather than waiting for proven returns—a faith-led adoption strategy carrying both opportunity and risk.

This pattern reflects several forces: competitive pressure to demonstrate AI adoption regardless of readiness, board-level expectations for AI strategy articulation, genuine recognition that manual identity governance cannot scale to 100:1 machine-to-human ratios, and hope that AI will address talent shortages.

The more sustainable path: pragmatic AI adoption starting with high-value, measurable use cases (behavioral analytics, risk-based authentication, automated provisioning) before tackling complex analytical functions requiring mature data foundations. Organizations treating AI as long-term capability building rather than near-term magic will see better returns.

The non-human identity challenge is finally getting strategic attention

With machine identities outnumbering humans by 100:1 or more, organizations recognize workforce identity management represents only a fraction of the actual identity security challenge. Budget and attention are finally shifting to address this explosion, with 36% prioritizing non-human identity security for 2026.

However, only 12% have achieved comprehensive automated life cycle management for machine identities. The remaining 88% rely on manual or ad-hoc processes that cannot scale. This creates a dangerous gap between recognition and capability. Organizations understand the NHI challenge intellectually but haven't yet built operational maturity to address it effectively. The next 18–24 months will reveal whether organizations can close this gap through investment and architectural change, or whether machine identity sprawl will continue outpacing governance capability.

Talent scarcity is reshaping strategy more than any technical factor

Perhaps more than machine identity explosion, AI potential, or compliance pressure, the shortage of skilled IAM professionals is driving consolidation, automation, and AI adoption decisions. Organizations can't hire their way out of complexity, so they must simplify.

This transforms how organizations evaluate identity security investments. Traditional ROI calculations emphasized cost savings and security improvements. Modern calculations must factor in whether proposed solutions increase or decrease skill requirements, whether they enable smaller teams to accomplish more, or whether they build or erode institutional knowledge. Investments requiring scarce expertise face higher bars for approval regardless of technical merit. Solutions enabling teams to do more with constrained resources get prioritized even if absolute costs are higher.

Identity security imperatives:

ManageEngine's recommendations for 2026 and beyond

Automate what can scale. Machine identity life cycle management, routine access reviews, anomaly detection, provisioning/deprovisioning: these cannot remain manual processes at current scale. Organizations managing 100:1 or 500:1 machine-to-human ratios need automation not for efficiency but for survival. Manual processes don't scale to these volumes, no matter how many people are hired.

Consolidate what must endure. Core identity infrastructure requires stability and reduced complexity. Organizations cannot afford perpetual integration maintenance, vendor coordination overhead, and architectural fragmentation when teams are already underwater. Consolidation creates foundation enabling everything else, viz., AI adoption, automation deployment, and Zero Trust implementation, to succeed.

Equip teams to do more with less. Whether through AI augmentation, process automation, or simplified tool sets, security teams need leverage. They cannot be trapped in vendor coordination, integration troubleshooting, and administrative overhead when threats evolve faster, attack surfaces expand broader, and compliance demands intensify. Architecture should multiply team effectiveness, not divide attention across complexity.

Internalize non-human identity governance as foundational, not ancillary. With 89% managing 25:1+ ratios and only 12% achieving automated life cycle management, the gap between challenge and capability is enormous. Organizations must shift budget, attention, and architectural thinking to address NHI explosion. This isn't supplementary to workforce IAM; at current ratios, it's the primary challenge.

Approach AI as augmentation, not automation run wild. AI will enhance expertise, not replace it, because the expertise doesn't entirely trust it yet, and that skepticism, born from operational reality rather than theoretical concern, will likely prove wise. Organizations deploying AI to extend human capability while maintaining oversight

will see sustainable returns. Those pursuing AI as excuse to eliminate expertise will face weaknesses when systems encounter situations outside training parameters.

Recognize that simplification doesn't mean uniformity. The goal isn't a single vendor for its own sake; it's operational efficiency, security effectiveness, and team sustainability. Some organizations may need hybrid approaches, maintaining specialized tools for genuine requirements while consolidating where possible. Pragmatism should guide decisions, not dogmatism about fully consolidated or best-of-breed.

Act with urgency, execute with persistence. Machine identity explosion, talent shortages, and operational burden from fragmentation create compound pressure that incremental improvement cannot address. Fundamental architectural change is necessary. However, transformation takes time, carries risk, and demands capabilities many organizations are still building. Organizations moving decisively while maintaining discipline to execute in measured phases preserving operational stability will succeed.

Survey methodology and demographics

The *Identity Security Outlook 2026* survey was conducted in October and November of 2025 to capture strategic thinking and investment priorities of identity and security professionals across North America (the US and Canada) as they plan for 2026 and beyond.

This report synthesizes survey findings with expert analysis, industry context, and strategic recommendations to provide identity security leaders with actionable intelligence for 2026 planning. The analysis deliberately examines not just what organizations are doing but why they're doing it, what barriers they face, and what questions they should consider as they navigate identity security's defining paradigm shift.

The report format prioritizes accessibility for busy security executives while providing sufficient depth for those seeking detailed understanding. Key findings are highlighted visually and summarized concisely, while extended analysis explores implications, answers difficult questions, and provides nuanced perspective on complex trade-offs organizations face.

- **Survey scope**
  The research examined machine identity proliferation, AI adoption patterns, identity stack fragmentation, consolidation sentiment, budget outlooks, and strategic priorities shaping identity security investments.

- **Participant qualification**
  Respondents were required to hold decision-making, influencing, or active implementation roles in IAM, PAM, or broader identity security strategy within their organizations.

- **Respondent profile**
  - 54% director-level or above
  - 51% from organizations with over 250 employees
  - 57% from organizations generating over $100 million in annual revenue
  - Diverse industry representation across IT, finance, healthcare, education, legal, and other sectors

About the author

Helen Yu is a Global Top 20 thought leader in 10 categories, including digital transformation, artificial intelligence, cloud computing, cybersecurity, internet of things, and marketing. She is an independent board director who brings unique perspectives to the board room, combining deep technology thought leadership, AI and cybersecurity risk management, go-to-market strategy, and the voice of the customer to deliver thoughtful questions and insights that drive informed decisions.

Helen has demonstrated success in leading ambitious companies with culture-building, multi-billion dollars revenue growth and profitability through a career spanning early-stage startups, pre-IPOs, and Fortune 500 enterprises, including Oracle, Adobe, and Marketo. She's managed over 100 million in profit and loss at a global scale.

With over 20 years of executive leadership, Helen has navigated organizations through digital transformation, strategic planning, AI and cybersecurity risk mitigation, go-to-market optimization, and financial oversight across various industries, including technology, manufacturing, insurance and financial services. With deep expertise in these areas, she draws upon a wide range of strategic and functional experiences to collaborate effectively and engage with fellow board members and senior management.

https://www.linkedin.com/in/yuhelenyu/

ManageEngine
PAM360

Unified PAM platform for modern enterprises