2026

OAK



THE VOICE OF 200 CISOS: **WHAT SECURITY LEADERS REVEAL ABOUT THE LIMITS OF IDENTITY SECURITY.**



THE VOICE OF 200 CISOs: WHAT SECURITY LEADERS REVEAL ABOUT THE LIMITS OF IDENTITY SECURITY.

Original research with CISOs and identity practitioners, by Oak
January–September 2026

The voice of 200 CISOs: What security leaders reveal about the limits of identity security 01

Executive summary 02

Key findings 04

Why we started listening 06

About the research 07

Where identity breaks 09

The new standard for identity security 15

Conclusion: Change the model, not the layers 17

EXECUTIVE SUMMARY

Organizations have invested more in identity than ever, but still can't govern access with confidence.



Across 201 in-depth interviews with CISOs, IAM leaders and security practitioners:

- **Visibility was the most common problem by far.** Half of all interviews (51%) raised incomplete visibility into identities and access.
- **Coverage is incomplete.** More than a third (38%) described applications their identity program can't reach.
- **Non-human identity gaps and visibility gaps go hand in hand**. More than a third of interviews (37%) raised non-human identity governance gaps, and two-thirds of those (67%) also raised visibility problems.
- **Manual work fills the gaps.** One in three interviews (34%) described recurring manual work, and nearly as many raised difficulty maintaining appropriate access (32%).
- **None of the top ten problems is niche.** Every one of the top ten problems came up in at least one in five interviews, including concern about trusting automated changes (20%).

What it costs

The burden shows up in time and people. Participants described one data-platform connector that took seven to nine months and a single HR integration taking ten. One 13-person security team dedicates a full-time person just to administer one governance tool. One airline's quarterly access reviews take six to eight weeks of preparation.

These organizations still struggle to build a complete picture of identities, access and risk across their environments and to answer the basic question:

Who, or what, can access what, right now, and why?

These aren't isolated problems. They point to one underlying problem: organizations can't govern access with confidence because they lack complete, current context. Tools that show more access may offer broader visibility, but still leave teams to do the work of fixing what they find.

Teams are left to reconstruct the relationships between them through integrations, spreadsheets, tickets and manual investigation. Adding another layer can address a specific gap without resolving the fragmentation underneath it.

AI raises the stakes on both sides. Agents act with greater speed and autonomy, often through permissions inherited from people and machines. At the same time, AI can make it possible to govern continuously: correlating context, analyzing access, and reducing the manual work required to keep governance current.

Gartner forecasts identity and access management spending will grow from $18.7 billion in 2024 to $29 billion by 2029. Yet, across our research, the gaps persist.

Five priorities emerge for the next chapter of identity security:



01

Rethink the operating model, not just the layers.

Adding another view on top of a fragmented stack adds visibility without adding control. Reviewing, granting and removing access should all work from one connected picture of every identity, application and permission, so that understanding and action happen in the same place.

02

Close coverage gaps, starting with one high-value use case

Not every program needs to start from scratch. Choose one problem that the current program doesn't solve well, such as just-in-time access or reviews for the most sensitive applications. Prove the result in access removed and hours saved, then expand.

03

Make least privilege the standard, and make it safe.

Keep access aligned with what the business actually needs without making security teams choose between reducing risk and disrupting work. Once agents inherit that access, every excess permission becomes a more urgent risk.

04

Govern agents as part of the identity program.

Human, non-human and agent identities require connected access and accountability, even when their controls differ. Access decisions need to account for context and intent at the moment of action.

05

Ground AI in complete identity data.

With complete, connected identity data, AI can take on the evidence-gathering and follow-up that consume identity teams, showing why each decision was made and confirming every change.

Together, these priorities point to a higher standard: identity governed as one connected, continuously understood system rather than a collection of separate controls.

Where the current IGA handles the basics well, start with priority 2. Where it has become the constraint, priority 1 comes first.

KEY FINDINGS

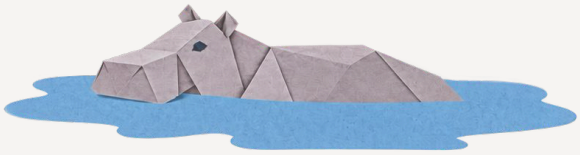
Incomplete visibility was the most frequently discussed challenge, raised in 51% of the interviews. But the findings show that the problem extends across every stage of governing access: discovering it, understanding what it allows, determining if it's appropriate, changing it and confirming the change actually happened.

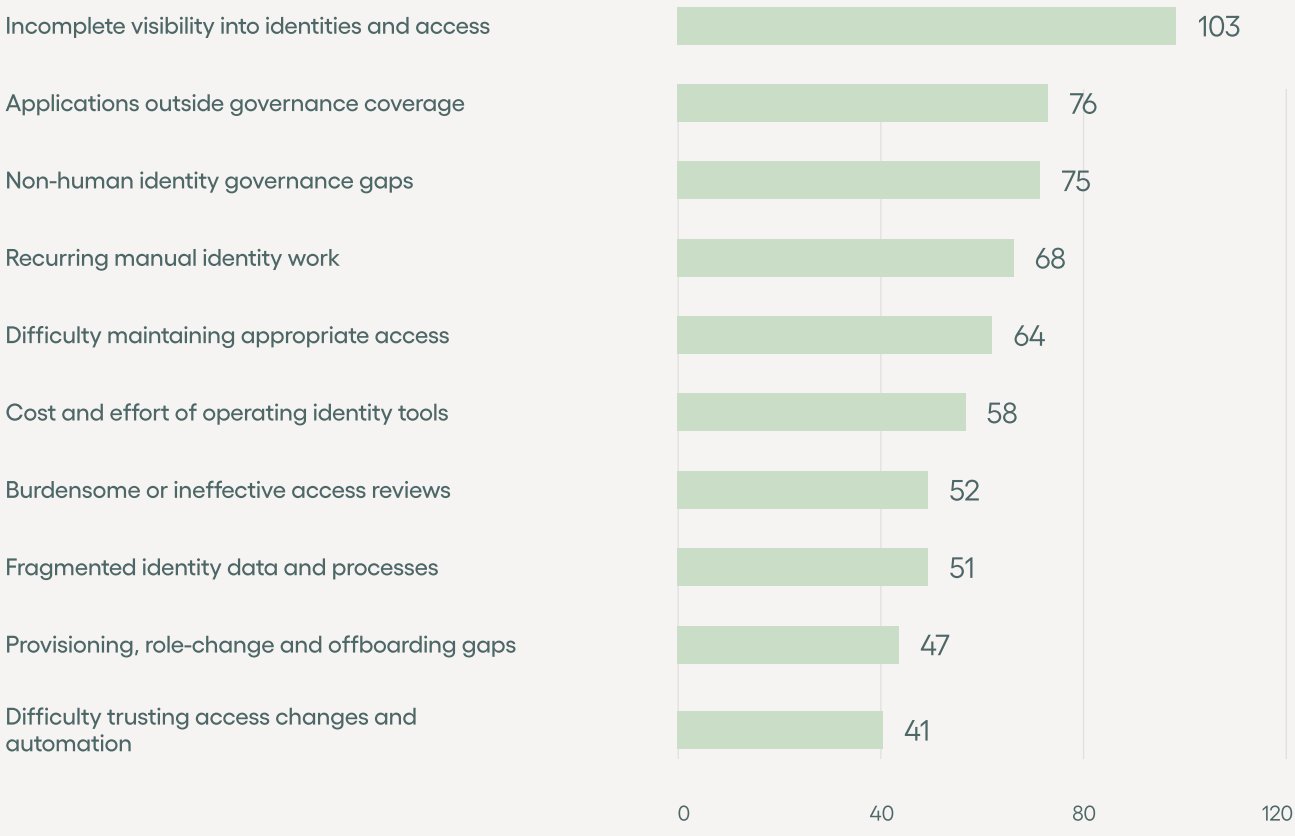
Organizations can have substantial identity infrastructure in place and still lack the context and control required to govern access confidently.

01/ THE PROBLEMS PARTICIPANTS RAISED

Visibility leads a wider governance problem

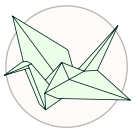
Supporting conversations, out of 201 analyzed conversation groups





*Themes overlap. Counts indicate documented support, not market prevalence or severity.

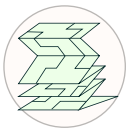
What the pattern tells us



01

Coverage and understanding are different gaps.

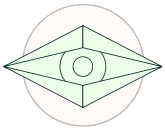
An application can be connected while nobody knows what its access allows.



02

Manual work is a sign of fragmentation.

Spreadsheets, tickets and custom scripts are how teams rebuild missing context.



03

Finding risk and controlling it are different problems.

Identifying a risk doesn't mean it can be immediately remediated.



04

Agents raise the stakes.

They move fast and unpredictably, making existing gaps more urgent.

One Underlying Limitation

Across these findings, the same limitation appears repeatedly: **organizations struggle to govern access with confidence because they do not have a complete, current and actionable picture of access across systems.**

CISOs and identity practitioners described the limitation from different sides.

CISOs focus on cost and confidence: the staff time lost to manual work, exposure in audits and uncertainty about who can really access what. Practitioners described the mechanics underneath: applications that are hard to connect, records that need to be reconciled, missing context and changes that depend on other systems.

WHY WE STARTED LISTENING

We kept hearing the same frustration, from very different organizations. Large enterprises with mature programs, experienced teams and established tools still ran access reviews on spreadsheets and had applications sitting outside governance. Smaller teams, often just one or two people responsible for identity, described the same gaps from the other side: too few hands, scripts only one person understood, and no time to look beyond the next audit. And across both, nobody could say with confidence which agents were running or what they could reach.



That didn't fit the usual explanation that these organizations simply needed more tooling, or more people. We wanted to hear, in their own words, what happens between a finding and a fix, what eats up their team's time, and how the rise of agents is shifting where identity teams focus.

We set out to understand three things:

01

Where identity governance breaks down in practice

02

What it costs the teams running it

03

What it would take to fix it.

ABOUT THE RESEARCH

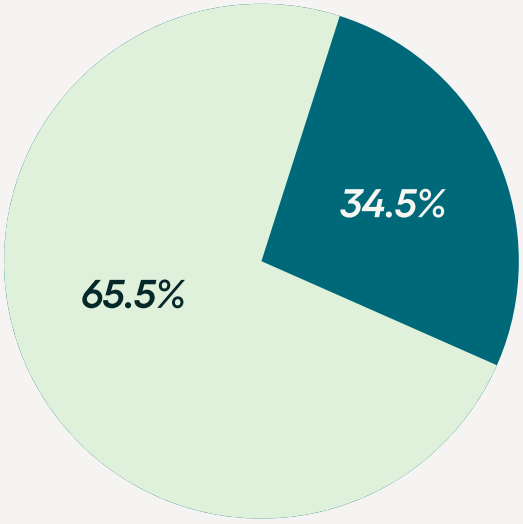
The research draws on 201 interviews with 93 organizations, held over eight months between January and September 2026. No surveys or questionnaires were used, findings come directly from what participants described in their own words.

Interviews ranged from exploratory interviews about identity challenges to in-depth reviews of participants' current identity programs and tools, discussions of implementations and operations and advisory sessions with experienced practitioners.

Participants included CISOs and other security executives, IAM leaders, security architects, engineers, IT leaders with identity responsibilities, governance practitioners and experienced advisors.

Who we spoke with

201 interviews with security and identity leaders



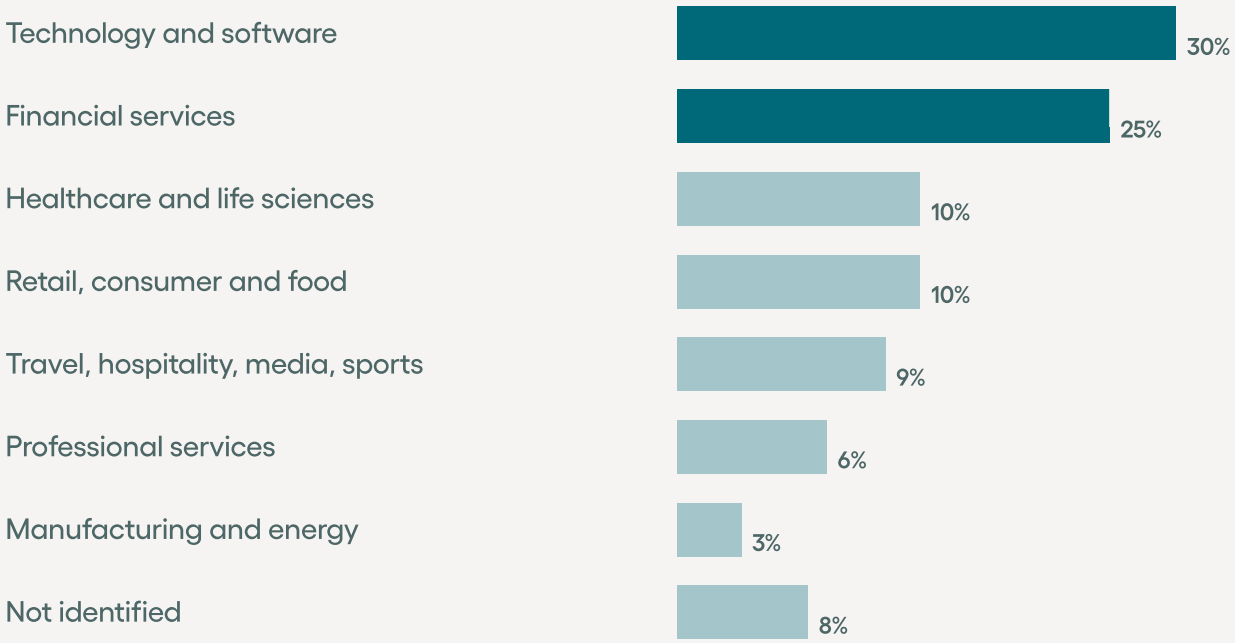
AMONG IDENTIFIED PARTICIPANTS

- CISOs, CSOs or Deputy CISOs
- IAM leaders, architects, engineers and practitioners

Participants represented financial services, healthcare, technology, retail, manufacturing, hospitality, sports and professional services.

Industry

Share of 93 organizations



Their starting points varied significantly: some were small teams establishing governance, larger programs extending established controls, and mature environments carrying significant customization and integration work. Organization size alone did not explain maturity. Both newer and established programs described gaps between the controls they wanted and what they could sustain.



Attribution and disclosure

Quotes are attributed by role, industry and company size, with names omitted. This research was conducted by Oak, which develops identity security software. The findings describe what participants said, and are not an evaluation of any product, including Oak's.

WHERE IDENTITY BREAKS

Five recurring themes emerged.

Each describes a different point where identity programs struggle to translate available data and controls into a dependable understanding of access.

01	× Visibility does not explain access
02	× Heavy investment hasn't reduced the operating burden
03	× Finding risk doesn't mean fixing it
04	× Agents turn an unsolved problem into an urgent one
05	× Least privilege is still aspirational

One problem runs through all five: organizations can't govern access with confidence because they lack complete, current context.

Theme 01

Visibility doesn't explain access

Incomplete visibility came up in **51%** of interviews, and application coverage gaps in 38%. Security leaders need more than an inventory of accounts. They need to understand who or what can access a resource, what that access allows, how it was granted and who is accountable. Limited visibility and incomplete application coverage leave those questions open.

> *"Our insight into who has access where is still very fragmented, even with a concerted effort over the last several months on it."*
>
> - CISO/CIO, education technology company with 1,000–5,000 employees

Evidence:

Applications the identity provider can't see. An application may technically be connected while ownership, access data or the authority to determine appropriate access remains unclear. One energy CISO described teams signing up for SaaS apps that the identity provider "*has no idea about*." Other applications are simply too old to connect.

One person can have several disconnected identities. The same person can accumulate multiple accounts, each with its own login, sometimes its own MFA, and sometimes none at all. Each tool may see its own account correctly but none sees the same person behind them, and that person's combined access is what actually matters.

Roles nobody can explain. Practitioners described situations where understanding an application role required contacting the vendor or building a test environment. Knowing someone has an admin role is not sufficient if nobody can explain what that role permits.



The limitation: seeing that access exists isn't the same as understanding what that access means.

Theme 02

Heavy investment in implementation hasn't reduced the operating burden

The cost and difficulty of operating and changing tools came up in 29% of the interviews.

Implementations take months or years, and the work doesn't end when they go live. Connecting applications, running reviews, and maintaining customizations become permanent jobs, even for small teams. One company spent ten months on a single HR integration. Another dedicated a full-time person just to administer a governance tool. Even mature programs described gaps filled with custom services that then have to be checked again at every upgrade.

Identity programs often *become* the work

Each quarterly access review campaign
Aviation

Learning to run a governance tool
Software

Waiting on one data-platform connector
Financial services

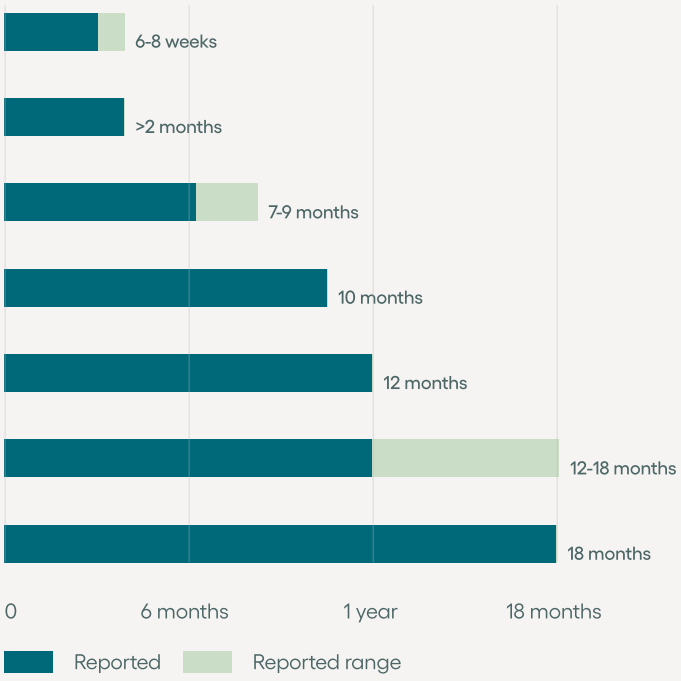
One HR system integration
Life sciences

A single entry point for all identities
Pharmaceuticals

Rolling out a new identity platform
Software

Connecting ~240 applications
Investment firm

Durations participants described for individual identity projects and tasks



"It took like a year, year and a half to get in... and it was one of our most expensive plays."

- CISO, describing a previous role at a software company with 1,000–5,000 employees.

"We've just gone through the pain to get in it."

- Global CISO, Fortune Global 500 life sciences company.

"We had a dedicated person, and all they did was user access reviews... wrangling Excel spreadsheets and emailing people. That's not a job for a human to do."

- CISO, media technology company with 1,000–5,000 employees, describing a previous employer

Evidence:

Governance becomes a full-time job. A 13-person security team dedicates one person full time to administering its governance tool. At one airline, access reviews run year-round, with weeks of preparation before each quarterly review.

Manual work fills the gaps. A global manufacturer relies on spreadsheets just to find out which users have MFA. At one energy company, a project manager tracks access reviews in a spreadsheet, triggered by a calendar reminder, and creates each one by hand.

Custom work never ends. Missing features are filled with add-ons and consulting hours which have to be maintained through every upgrade. One retailer described rewriting its identity platform "for like the fifth time."

The limitation: the people, time and custom work it takes to keep the tools running.

Theme 03

Finding risk does not mean fixing it

Recurring manual work came up in 34% of interviews, access-review burden in 26%, and lifecycle gaps in 23%.

Participants frequently described a separation between identifying inappropriate access and removing it. Tools may surface risky access, but addressing it requires a change in another system, made by another team. Until that happens, and until someone confirms it, the exposure remains.

"You know, honestly, it's chasing people."

- CIO, cybersecurity company with 1,000–5,000 employees

"It's completed when it's remediated."

- Security practitioner, consumer technology company with 1,000–5,000 employees

Evidence:

Identity work becomes detective work. Teams repeatedly described chasing owners, reconciling records and gathering context before they could make an access decision.

Role changes and departures leave residual access. When someone changes jobs or leaves, their primary accounts get updated but their access inside individual applications often remains. A food distributor said, "People change roles, and they maintain their privileges, and we have no idea."

Finding and remediation live in different systems. The tool that flags a risk usually can't fix it. Someone has to open a ticket, share it with another team and make the change in a separate system, all while the exposure stays open. An airline's head of IAM described two major identity platforms that "don't talk to each other," so a threat detected on someone's device doesn't change their access.

The limitation: the distance between finding a problem and actually fixing it and confirming it's been removed.

Theme 04

Agents turn an unsolved problem into an urgent one

Governance gaps involving service accounts, credentials, workloads and agents appeared in 37% of the interviews and among those interviewed:

67%
raised visibility problems

48%
raised appropriate-access problems

36%
raised lifecycle problems

People enter an organization through a process: HR creates a record, access is approved, offboarding removes it. Non-human identities never had that process. Service accounts and API keys are created as needed, often with no owner and no end date. Agents run on these same accounts and keys, inheriting whatever access they already have. Agents didn't create this problem, but they make it far more urgent.

"I'm sure our developers have created agents and they're running autonomously doing things that I don't know about."

— CISO, media technology company with 1,000–5,000 employees

"I think that this is just an extension of never managing non-human accounts correctly in the first place."

- CTO, Fortune 500 hospitality company

"We need something bigger, especially with agents being built that we don't know about."

- CISO, global manufacturing company, more than 10,000 employees

Evidence:

Machine identities were already difficult to govern. Service accounts and API keys were created without owners or lifecycles, and in many environments they now outnumber people. One practitioner found about 12,000 service accounts "before we had a single AI agent."

Agents inherit the existing access. An agent will take all of its owner's permissions, regardless of what the task requires. An IAM lead at an investment firm said, "if an agent is assuming my identity... say I have access to [our IGA] as an admin, the agent, which is impersonating me, can also create a user."

Accountability becomes harder to maintain. Agents are created outside any onboarding process and often outlive the people who built them. A travel platform described agents "with no lifecycle management and no ownership mapping."

The limitation: an existing accountability gap becomes far more consequential when identities can act autonomously.

Theme 05

Least privilege is still aspirational

Difficulty defining and maintaining appropriate access came up in 32% of interviews and concerns about trusting automated access changes in 20%.

Everyone agrees on the goal. The challenge is removing access without breaking the work people need to do. When nobody is sure what access is actually used, excess becomes the safer choice.

> *"People don't feel empowered to push back on access."*
>
> - Head of Security, software company with 501–1,000 employees

> *"If you try and rein them in, they go up to the management and complain."*
>
> -Security architect, pharmaceutical distributor, with 1,000-5,000 employees

Evidence:

Uncertainty favors excess access. When teams cannot confidently determine what someone needs, broader access becomes the safer operational choice - when nobody knows exactly what a person needs, the easy answer is admin.

Standing access is the default. Access granted once tends to stay, long after the need has changed. An AI company hiring 15-20 people a week said: "We have standing access right now - it's not how we can operate, realistically, as we grow."

Removing access is an organizational challenge. Questioning someone's access can create friction, especially with senior users. Practitioners described the need for confidence, evidence and graduated implementation before making changes.

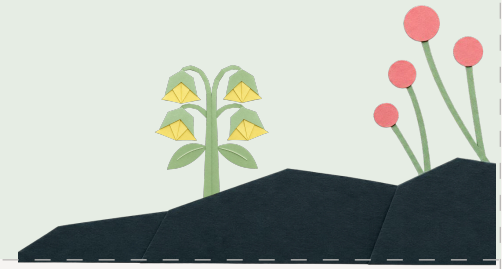
The limitation: the ability to make accurate, defensible changes without disrupting the business.

Industry Lens: similar gap, different symptoms

Industry groups are defined by the research team.

Financial services	**SaaS and third-party sprawl:** Identity reaches far beyond employees to contractors, advisors, and partners while thousands of applications can sit outside the identity provider.
Healthcare and life sciences	**Legacy systems and compliance burden:** Small teams carry heavy compliance demands, especially across clinical and ERP systems that are hard to integrate. Some review access for only a fraction of their applications.
Technology and software	**Scale and agents:** Rapid hiring makes standing access unsustainable, while agents are already reaching into HR and finance systems.
Travel, hospitality, media and sports	**Privileged and third-party identities:** The gaps sit at the edges: third parties, people with several admin accounts, and reviewers approving access for people who may no longer be on the team.
Retail, manufacturing and energy	**Legacy infrastructure and manual governance:** Critical access lives in legacy systems and disconnected directories and reviews are often tracked in spreadsheets.

THE NEW STANDARD FOR IDENTITY SECURITY



The research points to a higher standard: identity security that understands access across the whole environment, keeps that understanding current and turns decisions into confirmed change.

The five shifts below show what participants told us and what the research team believes it will take:

FROM	TO
✗ Disconnected controls	✓ Easier operating model
✗ Partial snapshots	✓ Complete, current context
✗ Separate identity categories	✓ Unified accountability
✗ Recurring manual work	✓ AI grounded in complete data
✗ Aspirational least privilege	✓ Safe enforcement

1. From disconnected controls to an easier operating model

What we heard:

Programs stitch together tools and every seam loses context. Even mature teams described coverage gaps, custom integrations and repeated rebuilds.

What it requires:

Identity security needs to connect people, non-human identities, agents, applications, resources, permissions, activity and controls into a coherent understanding of access without matching an increase in integration and maintenance work.

The test:

Does the program get easier to run as coverage grows, or harder?

2. From partial snapshots to complete, current context

What we heard:

Reviews capture access at one moment, then go stale as roles, permissions and projects change.

What it requires:

Context that stays current between reviews, reassesses access whenever relationships change, and keeps missing or outdated information visible.

The test:

Can we see every application that matters, and would our understanding of access still be accurate a month after the last review?

3. From separate identity categories to unified accountability, including agents

What we heard:

Agents may act through a service account, delegated user permissions, credentials and multiple applications and often outlive those who created them.

What it requires:

Understanding the full chain. Every identity should have enough context to establish what it represents, why it exists, what gives it access and who is accountable for it.

The test:

Can we explain an agent's access, identify who is accountable for it, and revoke it when its purpose ends?

4. From recurring manual work to AI grounded in complete data

What we heard:

Most identity effort goes into chasing owners, gathering evidence and confirming that approved changes actually happened.

What it requires:

AI that works from complete, connected identity data, so it can take on the recurring work, with clear approvals and proof that each change happened.

The test:

How much of the team's time goes into assembling evidence and is that number decreasing?

5. From aspirational least privilege to safe enforcement

What we heard:

Everyone wants least privilege. Uncertainty and the fear of disrupting work, keep standing access in place.

What it requires:

Clear reasons for removing access and what it will affect, changes made gradually, and confirmation that work continues. The goal is to continuously reduce access without slowing the business.

The test:

Can we remove unnecessary access, explain why, and prove nothing went wrong?

CONCLUSION: CHANGE THE MODEL, NOT THE LAYERS

This section reflects the research team's interpretation of the findings.

Each new identity tool may close one gap, but it adds another source of identity data and another system to maintain. Identity now runs as a stack of separate products, and teams are left to connect them by hand.

Security leaders are ready for change. Several plan to unify access reviews, rethink their governance platforms and bring agents into the scope next year.

The research points to two paths forward:

01. Start with one high-value use case

Choose a high-value, high-impact problem your IGA does not fully solve. Connect the missing data and context to get a complete view of the identities and access involved. With that full picture, act on the problem and measure the result: fewer hours of manual work, more applications covered, less unnecessary access. Once it proves it can reduce unnecessary access and manual work without disrupting the business, expand.

02. Change the operating model

When every expansion means another rebuild, another custom integration and another round of manual reconciliation, adding layers is not the answer. Changing the model means governing people, machines and agents as one connected system, where access is understood, decided and changed in the same place, and where the program gets easier to run as it grows.

Every gap in this report becomes more dangerous once agents are involved. Building a separate governance layer for agents would repeat the same fragmented approach, but with higher stakes. We believe the organizations best positioned for what comes next will be the ones that govern every identity in one model.

The question for every identity leader is simple: is our current approach getting easier to run as it grows, or harder? **If the answer is harder, the next chapter of identity security starts with the operating model, not another layer.**