DARKREADING
RESEARCH

JUNE 2025

# State of Identity Security Survey

Commissioned by SailPoint

# Executive Summary

As enterprises drown in a sea of new devices and identities, identity risk, and identity controls have grown so fragmented that it's hard to keep track of who oversees what pieces. This lack of consolidation and coordination in Identity and Access Management (IAM) has resulted in poor risk visibility and mediocre controls, all of which are making it hard for enterprises to excel at even the basics of entitlements management and effective access controls.

**These are the findings of the 2025 State of Identity Security Survey, which offered the following insights:**

### Biggest IAM Challenges

- 40% of organizations use four or more different identity products or platforms
- Just over 1 in 10 organizations use seven or more products

**24%**

**of organizations are highly confident in their ability to effectively manage entitlements and authorization**

### Who's in Charge of IAM?

There's no clear winner:

- 35% put CISO/CSO in charge
- 24% leave identity up to CIO
- 15% say CTO is in charge
- 10% have an IAM governance committee
- 39% of organizations have an identity team separate from security

**55%**

**of these separate teams don't have a close working relationship with security or the relationship is contentious**

### Contextualizing SecOps With Identity

- 30% of organizations reported they've suffered at least one identity-related breach in the past year
- Only 28% of organizations say their SOCs and incident responders have easy access into tools that offer a complete view of identity and access activity

**52%**

**of organizations say blurred lines of responsibility between identity, security, and SOC teams causes moderate to significant delays in response to threats with an identity component**

### IAM Reporting

- 42% of organizations don't report to the board on identity-focused risks or don't know whether they can report on those risks

**27%**

**of organizations track number of segregation-of-duty violations**

- Just 1 in 3 organizations track average time to deprovision accounts and access

### Automation and AI

- Only 12% of organizations say they are very automated in how they administer identity management and identity controls

## Biggest IAM Challenges

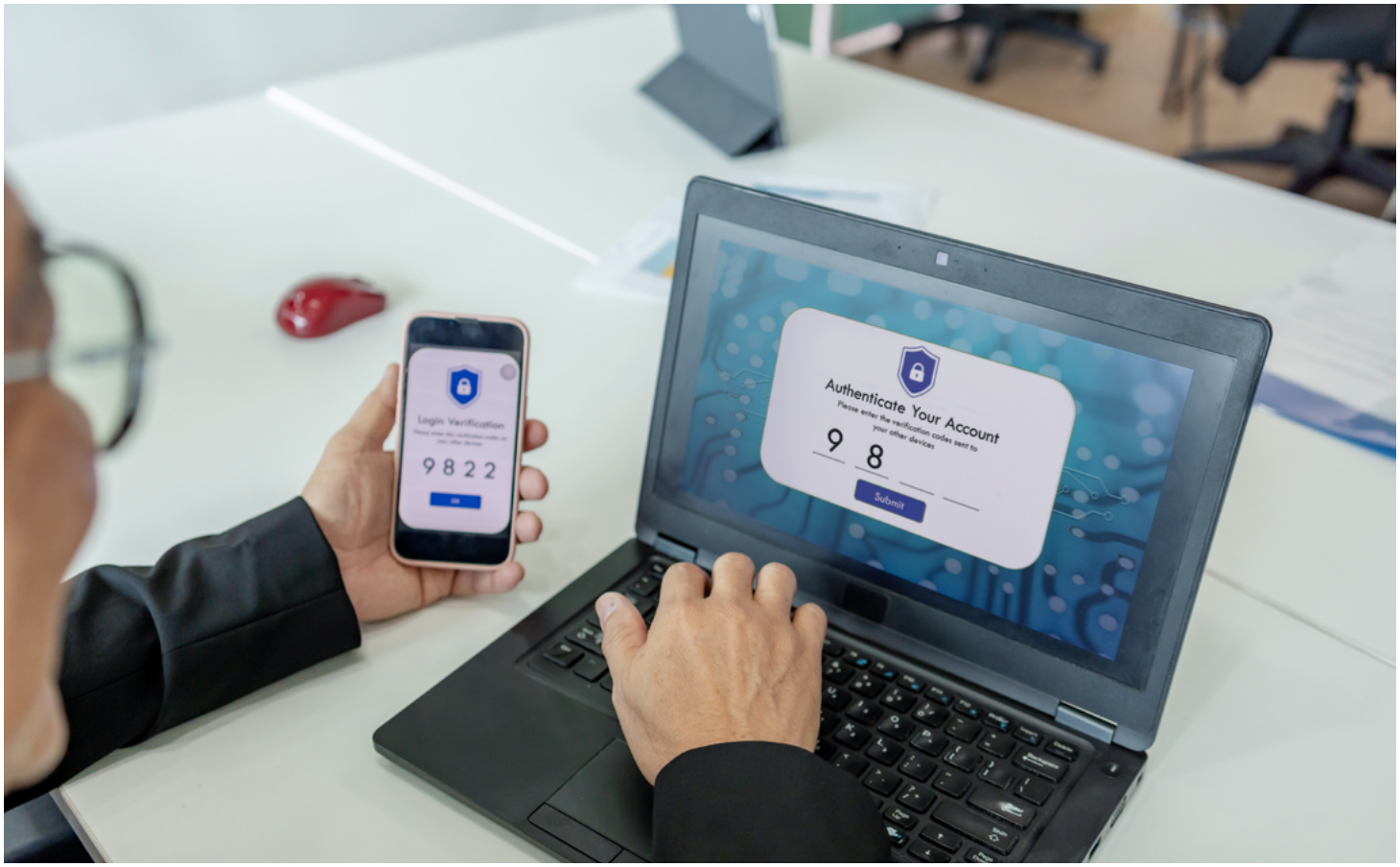
One of the biggest themes emerging from our State of Identity Security Survey is that IAM strategies, lines of responsibilities, and product usage are far from centralized. Many organizations today juggle a whole portfolio of IAM products that may or may not play nicely together.

Our study shows that 40% of organizations use four or more different identity products or platforms. More than 1 in 10 organizations say they use seven or more different identity products or platforms within their organization.

This inevitably leads to underutilized software and difficulty in coordinating IAM activities across different tools and different departments that run them. While we didn't follow up to ask about adoption rate or usage levels across these products, it's safe to speculate that, in some instances, these products are underutilized shelfware. But, in many cases, they are simply well-used products that may be serving a tapestry of varied departments and business units in slightly different ways. Regardless, the abundance of products frequently leads to (or is symptomatic of) a lack of cohesive orchestration of identity security strategy across an organization.

This is likely why many organizations struggle with identity security fundamentals like entitlement management, which survey results indicate is a major challenge. Only 24% of survey respondents say that they are highly confident in their ability to effectively manage entitlements and authorization. This reflects a glaring gap for the 3 in 4 other organizations that don't report this kind of excellence, as entitlements management is one of the basic building
blocks of effectively managing access.

There are a range of factors that make it difficult for organizations to meet these entitlement



management challenges. Many organizations struggle to gain a clear view of how identities are connected and the context in which they operate — especially as the attack surface expands and the number of systems requiring access control keeps ticking upward.

"My No. 1 challenge in managing entitlements is maintaining visibility and control over entitlements in a complex and dynamic environment," one respondent explained. "As organizations adopt cloud services, IoT devices, and remote work, the number of systems and applications requiring access control explodes. This expands the attack surface and makes it harder to ensure consistent security policies across all platforms."

The dynamic nature of managing entitlements and access was a recurring theme among those who offered free responses to the challenge question.

"Organizations are constantly changing. Employees join, leave, and move between departments," one security leader said. "New applications and resources are deployed. Entitlements need to be updated in real time to reflect these changes. Keeping entitlements synchronized with the current state of the organization is a continuous challenge."

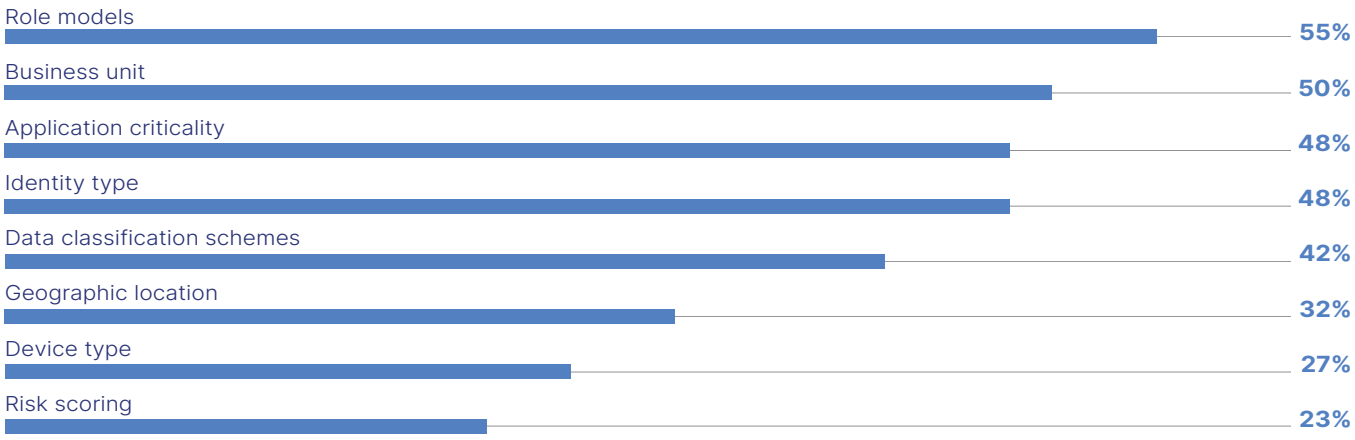
In the face of this dynamic environment, many organizations struggle to balance security needs with business agility. In many instances, this results in privilege creep as organizations don't have the processes or resources in place to claw back entitlements as employees move around within the organization.

"Over time, users accumulate unnecessary access rights due to role changes, temporary projects, or poor deprovisioning practices," one respondent reported.

*Figure 1*

**DETERMINING ACCESS**

**What contextual attributes do you use to determine access entitlements?**




Note: Multiple responses allowed
Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

Meantime, AI proliferation across the enterprise is further exacerbating many existing entitlement management practices and broadening identity security problems. The survey showed that 70% of organizations believe that increased AI adoption across the enterprise has had a moderate to severe impact on the exposure of identity infrastructure and access control.

One bit of good news is that a healthy 63% of organizations say they have the means to continuously evaluate access levels across users and groups when appropriate.

However, many of them still depend on very simple contextual attributes to determine access entitlements. For example, the top attributes used in entitlement management are roles (55%), business unit (50%), application criticality (48%), and identity type (48%) (**Figure 1**). Organizations are significantly less likely to include more risk-oriented attributes like geographic location (32%) or risk scoring (23%). This shows that many organizations still don't have the wherewithal to conditionally manage access levels based on more sophisticated risk factors

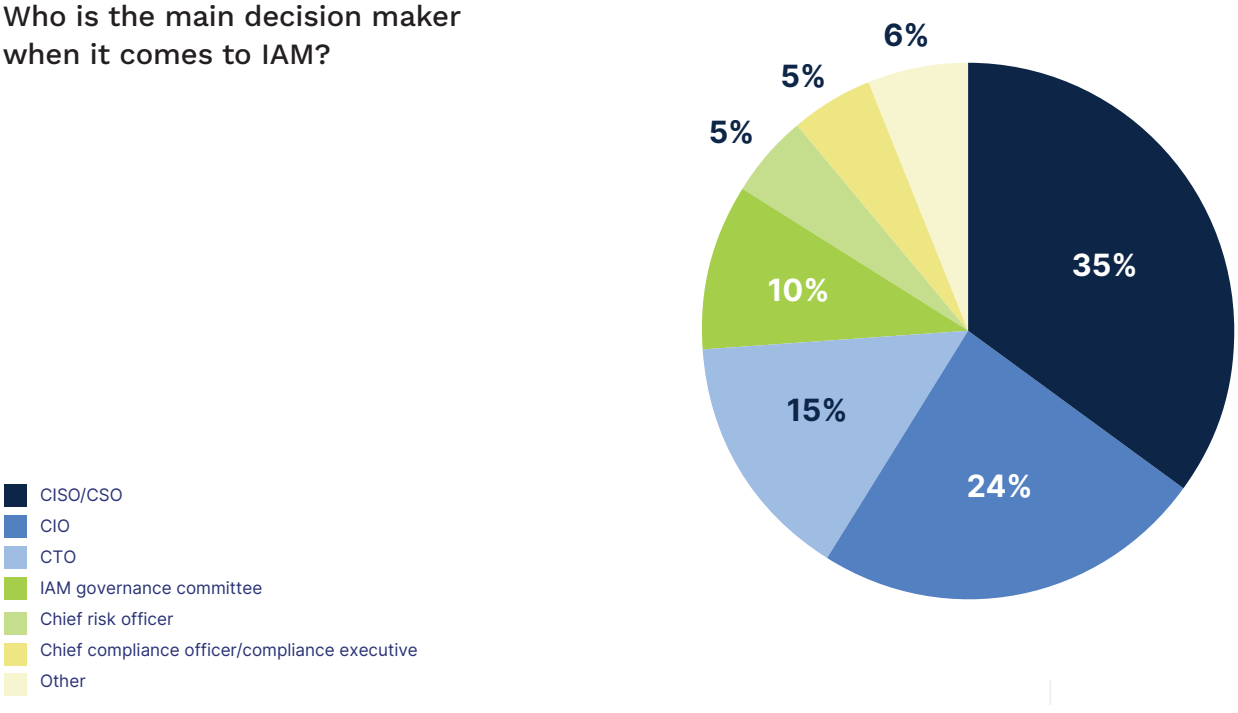
## Who's in Charge of IAM?

The fractured nature of identity security in the enterprise today is reflected in the fact that there's no real consensus about who should oversee IAM and identity security. Some 35% of survey participants say they have charged the security function — either CISO or CSO — as the buck-stops-here authority for identity. However, another 39% leave that authority to non-security tech leaders — either CIO (24%) or CTO (15%) (**Figure 2**). Finally, an additional 10% report that they have an IAM governance committee — typically comprised of both security and user-

*Figure 2*

**IAM DECISION MAKERS**

Who is the main decision maker when it comes to IAM?

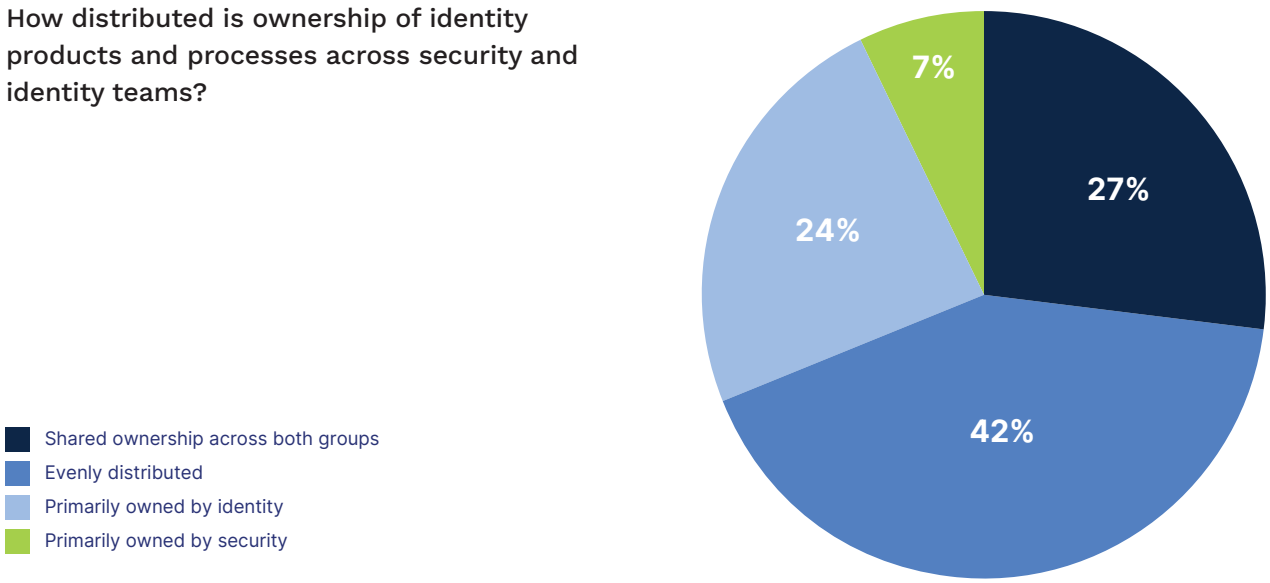



Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

*Figure 3*

**OWNERSHIP OF IDENTITY PRODUCTS AND PROCESSES**

How distributed is ownership of identity products and processes across security and identity teams?




Base: 40 respondents who have a dedicated identity management team
Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

experience/tech function stakeholders — making meaningful decisions about identity.

On the day-to-day and tactical front, almost 2 in 5 organizations have a dedicated identity management team outside of its security function that handles most identity management duties. Among those, 78% say that this separate team works very closely with the security team. But many of those that work closely with the security team don't do so harmoniously. The survey showed that 55% either don't have a very close working relationship with the security team or the relationship is contentious.

In the meantime, how are developers managing the relationship with those in charge of identity? Developers are tasked with building and updating identity functions and components within their software. Some 25% of organizations admit that the line of communication between identity/security teams and developers who are asked to update software to mitigate identity flaws or configuration risks are convoluted. Plus, only 26% say that communication is very clear and the collaboration is smooth. The bulk of organizations are somewhere in the middle, with 49% stating that communication is somewhat clear but there is some red tape involved.

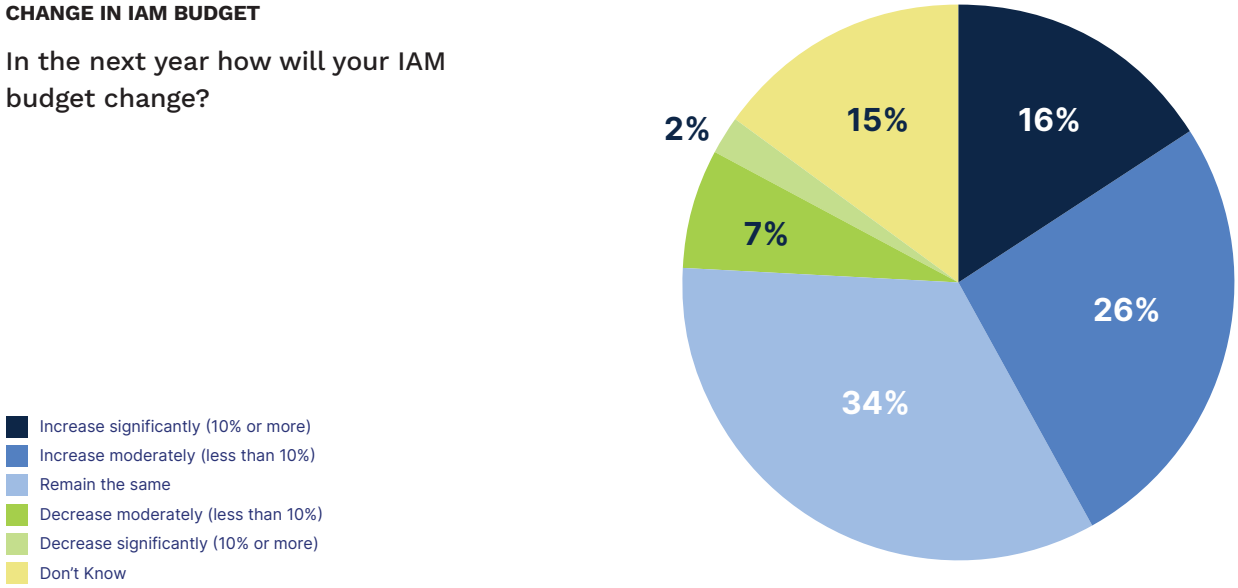
The fallout from this lack of harmony between identity teams, security teams, developers, and all the stakeholders in between can have a significant impact on the state of identity security in an organization. One of the biggest ones is a misalignment of priorities.

"The friction between identity and security teams often leads to significant gaps in identity security," one respondent wrote. "Identity teams focus on enabling seamless user access, ensuring availability, and reducing friction for employees and customers. While security teams prioritize risk mitigation, enforcing strict controls to prevent unauthorized access and breaches."

*Figure 4*

**CHANGE IN IAM BUDGET**

In the next year how will your IAM budget change?




Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

If there's no effective coordination of which stakeholder's priority 'wins' in any given situation, organizations will struggle to control identity and access in a coordinated and risk-managed fashion. This can become especially apparent during incident response and crisis situations.

It's hard to say whether the murkiness of who is in charge leads to confusion about who oversees paying for what — or vice versa. Regardless, our data shows that there's a wide range of investment strategies, spending patterns, and priorities for IAM budget out in the enterprise today.

When asked where identity spending comes from, answers tracked closely with the percentage of organizations with separate identity teams. Thirty-five percent say the identity budget is separate from the security budget.

Another 21% don't know or are unsure — which indicates how siloed many identity portfolios can be at organizations that don't have clear policies and directives about who is ultimately responsible for identity management work.

Diving into the distribution of ownership of identity products and processes, a majority (69%) said it was either shared ownership or evenly distributed where security owns some and identity owns others (**Figure 3**). When a single group had ownership, that was typically the identity group. Nearly a quarter of those organizations with a separate identity organization said that their organization also has sole ownership of identity products and processes.

A plurality of respondents (42%) say that regardless of its departmental source, their IAM budget will increase in the coming year, with 16% saying it will increase significantly by 10% or more (**Figure 4**). Another 34% say it will stay the same. So, investments are accelerating.

The top three IAM/identity security investments in the next year are:

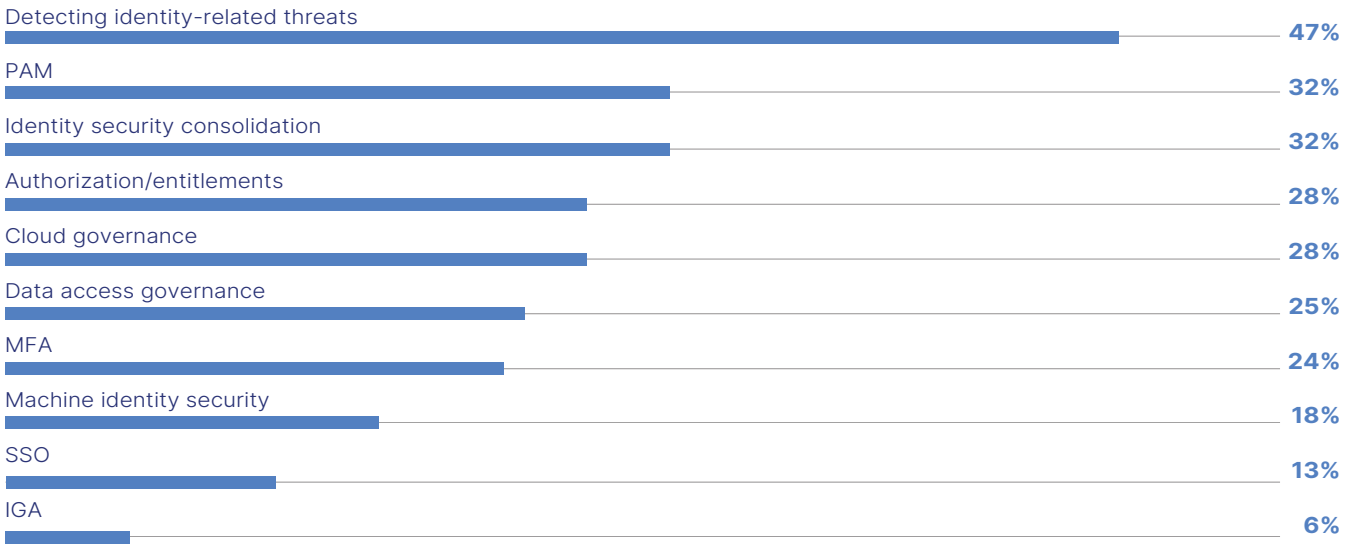
- Detecting identity-related threats (47%)
- PAM (32%)
- Identity security consolidation (32%) (**Figure 5**)

Many organizations didn't rate longtime budget priority staples like MFA (24%) or SSO (13%) as big

*Figure 5*

**FOCUS OF IAM INVESTMENTS**

**What will be the focus of your biggest IAM/identity security investments in the next year?**




Note: Maximum of three responses allowed
Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

investment focuses — likely because they've already poured money into these areas over the last few years and are now free to tackle more complex identity problems.

## Contextualizing SecOps With Identity

The lack of coordination and prevalence of identity security siloes across the enterprise creates many obstacles for security operations teams who would like to more completely weave intelligence about identity into detection and response activities.

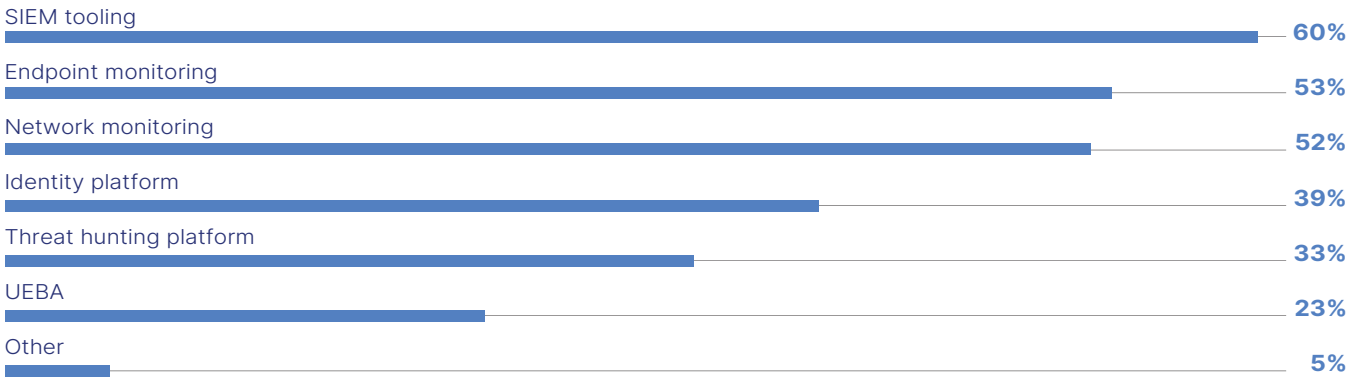
As stated earlier, the survey found that 30% of respondents reported experiencing at least one identity-related breach or major security incident in the past year, while another 18% were unsure. This uncertainty suggests that the actual number of affected organizations may be higher than reported. Our survey shows that organizations constantly struggle to provide security operations and incident response teams with meaningful identity data that connects flaws and threats to broader security data. In many ways, it is a 'we don't know what we don't know' situation when it comes to identity threats. SOC and incident response teams struggle to gain meaningful visibility into identity and access activity to help contextualize their response to security threats. Only 28% of organizations say they have easy access to tools that offer a complete view of identity and access visibility.

As a result, they're relying on what security information and event management (SIEM) platforms, endpoint monitoring, and network monitoring tools can tell them. When asked how they identify access outliers and anomalous log-in behavior, 60% said SIEM, 53% said endpoint monitoring, and 52% said network monitoring (**Figure 6**). Far fewer, only 39%, say they use identity

*Figure 6*

**IDENTIFYING ACCESS OUTLIERS**

**How does the SOC team primarily identify access outliers and anomalous login behavior?**




Note: Multiple responses allowed
Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

platforms for their work, and just 23% use user and entity behavior analytics (UEBA).

It's hard to say if it is a product-driven chain of responsibility or if the tooling is shaped by organizational structure, but many security operations teams, whether SOC or incident responders, are disintermediated from identity-related risk mitigation. Approximately 43% of organizations report that either identity management staff, security staff outside the SOC, or other IT teams end up doing remediation and response when identity-related risks or problems crop up from a flaw or active incident (**Figure 7**).

This only serves to further blur the lines of responsibility of who oversees identity — whether during the normal day-to-day grind or in the middle of a crisis. These blurred lines of responsibility between identity/security/SOC inevitably cause at least some kind of delay in response to threats with an identity component. Over half — 52% — say these delays are moderate to significant.

## IAM Reporting

The fractured nature of identity security responsibilities and how it is operationalized in the enterprise bubbles up into strategic reporting capabilities and audit readiness as well. Even though identity security is core to defending against some of the biggest threats to the enterprise, and access control and entitlement management is at the nexus of nearly every meaningful cyber-risk control, many organizations lack in-depth reporting around identity risks.

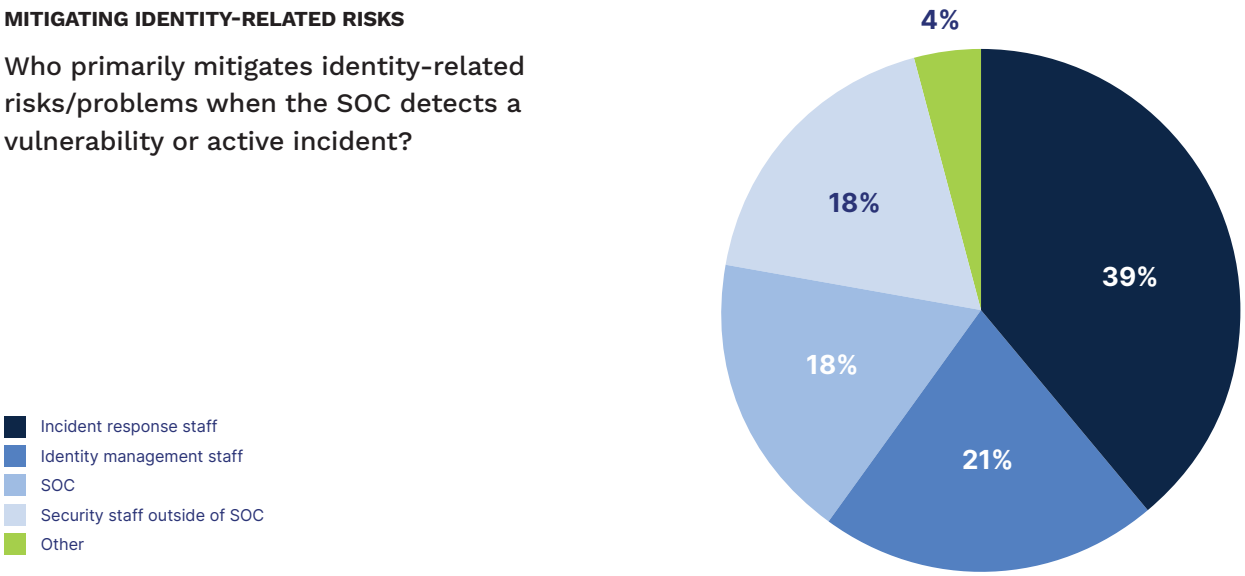
A full 42% of organizations either flat out admit they don't report on identity-focused risks or don't know whether they can report on those risks to business stakeholders. Meanwhile, 50% say they don't have (or don't know whether they have) an easy way to visualize or report on identity risk levels.

Even when organizations measure and report identity risks to the business, the KPIs they track against are not very effective at aligning with the risks. The top three most common KPIs were the

*Figure 7*

**MITIGATING IDENTITY-RELATED RISKS**

Who primarily mitigates identity-related risks/problems when the SOC detects a vulnerability or active incident?

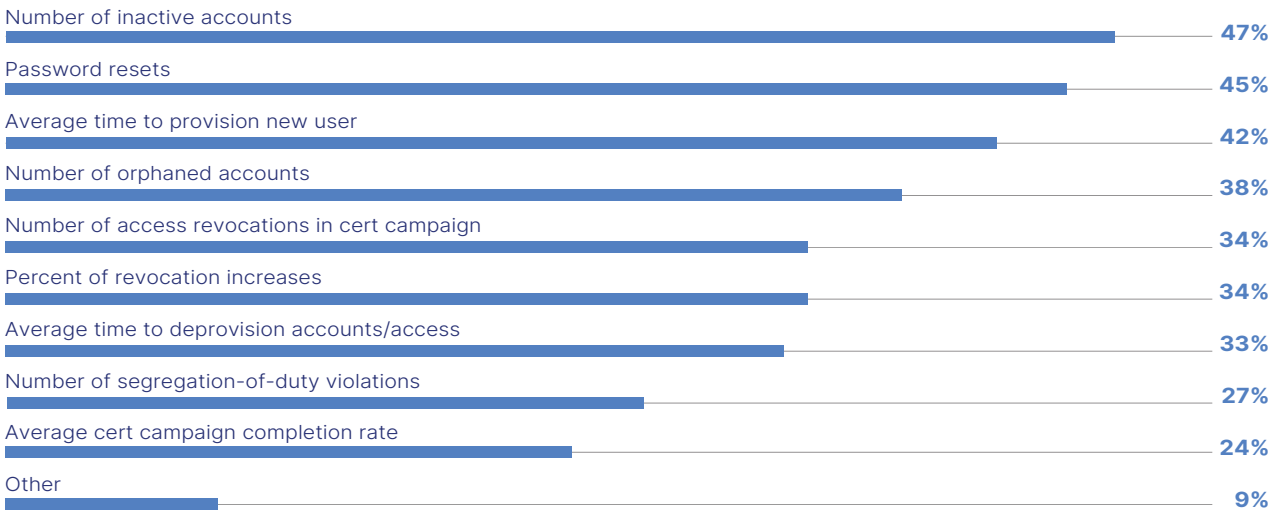



Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

*Figure 8*

**KPIS**

Which KPIs do you use to measure and report risk to the business?




Note: Multiple responses allowed
Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

number of inactive accounts (47%), password resets (45%), and average time to provision new users (42%) (**Figure 8**).

At the same time, KPIs that directly impact risk are much less likely to be tracked. For example, only 27% of organizations track the number of separation-of-duty violations and just 33% track average time to deprovision accounts and access.

This lack of identity security reporting and visibility makes it extremely difficult for organizations to prepare for audits and meaningfully manage identity risk.

## Automation and AI

Finally, visibility and reporting aren't the only major obstacles to efficiently managing identity risk. Many organizations also struggle to handle the scale of IAM because they've not been able to effectively automate the growing crush of administrative and strategic duties involved in modern identity security.

Only 12% of organizations say that they are very automated in administering their identity management and identity controls. A significant segment of organizations remain highly or primarily manual, with almost 1 in 5 organizations admitting to that level of manual work. The majority say they are somewhat automated.

Though we didn't follow up with a question on what percentage of automation they use across the entire breadth of their identity work, we did ask respondents to rank common IAM admin tasks from most to least automation.

The top three activities were password management/password resets, onboarding/offboarding, and permissions entitlement management (**Figure 9**). The more complex and time-consuming duties around reporting and separation of role modeling and role creation ranked lowest.

*Figure 9*

**AUTOMATION OF IAM TASKS**

**Please rank the following IAM administrative tasks from most automated to least automated.**

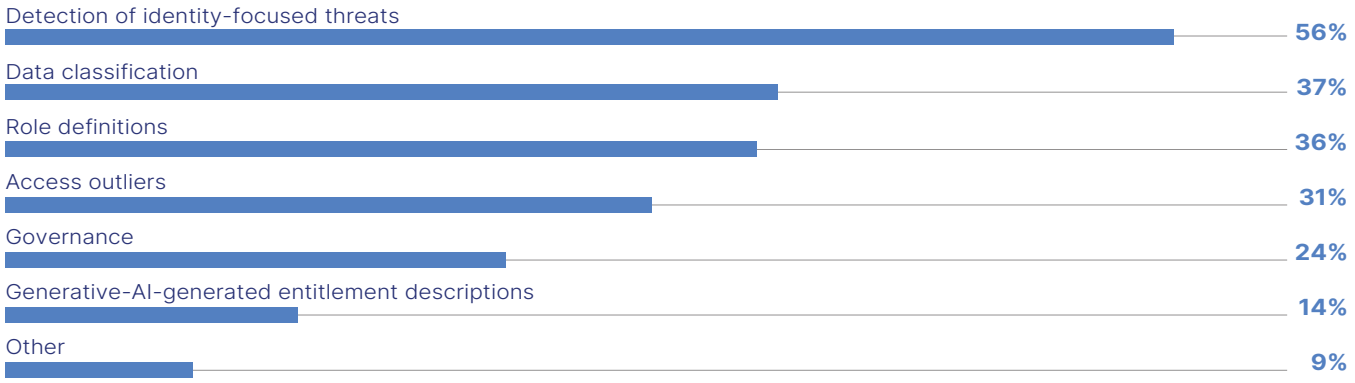
| | Overall Rank | Score |
|---|---|---|
| Password management/password resets | 1 | 433 |
| Onboarding/offboarding | 2 | 422 |
| Permissions/entitlement management | 3 | 369 |
| Access requests/refusals | 4 | 356 |
| Access certifications/access review | 5 | 339 |
| Reporting | 6 | 304 |
| Separation of role modeling and role creation | 7 | 254 |

Note: Rank is based on a weighted score. Responses are weighted, and scores represent the sum of all weighted counts.
Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

*Figure 10*

**IMPROVEMENT OF IDENTITY SECURITY DUE TO AI-DRIVEN IAM TOOLING**

Which areas have AI-driven IAM tooling improved identity security in the past two years?




Note: Multiple responses allowed
Data: Dark Reading survey of 108 senior-level cybersecurity professionals with 500 or more employees, March 2025

Many organizations are hopeful that AI-driven IAM can help improve administrative tasks and smooth the divide between identity and security operations. In the past two years, the most impactful improvements they've seen from AI-driven IAM tooling are around the detection of identity-focused threats (56%), data classification (37%), and role definitions (31%) (**Figure 10**).

## Conclusion

Navigating the challenges and opportunities identified in this year's State of Identity Security Survey will be no easy feat. Developing and executing a comprehensive strategy will require investment in consolidating tooling, improving automation, and encouraging collaboration between all stakeholders impacted by identity risk. The following are four best practices that identity security leaders should consider as they seek to improve their capabilities.

### Appoint an executive sponsor

One of the biggest reasons identity strategies have remained so fractured across enterprises is that it's still largely viewed as a nitty gritty operational detail with little executive relevance. However, ask a CEO how unimportant these decisions are in the wake of a business email compromise (BEC) attack, and it becomes very clear how pivotal access controls are to risk postures. Appointing an executive sponsor can go a long way to ensuring that organizations can glue together all of the pieces of their identity strategy under a single strategic banner. Strong executive guidance can establish clear lines of accountability and provide direction, support, and advocacy. This might also go a long way towards bridging the communication barriers between the identity team and the security team.

### Maintain good data hygiene with effective data access controls

Organizations face significant fines, brand damage, and other penalties when they are found to be out of compliance with regulatory requirements — consider the $52 million fine from the FTC lobbied against Marriott last year as a prime example. Whether for lapses in data security (preventing unauthorized access to data and protecting it from threats and breaches) or data

privacy (concerned with how data is collected, used, stored, shared, and destroyed throughout the entire data lifecycle), the consequences can be daunting. Data access controls enable you to restrict access (e.g., enforce least privilege) based on a set of policies that prevent sensitive information from getting into the wrong hands. You can tighten access controls by removing overprivileged or dormant access, monitoring for malicious activity, and automatically taking corrective action in real time.

## Continuously monitor and audit access

Having a regular schedule of certification reviews and utilizing AI access recommendations will mitigate overprovisioning, increase revocations, and save on licensing costs.

Being able to identify anomalous access is vital for an effective identity security program. Outliers can do serious damage if not discovered quickly. By automatically flagging anomalies, outliers help identity teams quickly pinpoint potential security risks or compliance violations, enabling faster response, and reducing the threat surface.

## Leverage automation and AI to reduce manual, repetitive tasks

Organizations simply cannot manually keep up with the dynamic and rapidly growing identity landscape. To modernize, enterprises need an automation-first stance to all things identity-related.

Automated user provisioning follows rules created for accounts, onboarding and offboarding new users with what they need to perform their role from day one — and removing or adjusting that access on their last day or when they change roles. This improves the user experience and reduces the use of shadow IT while reducing the burden on HR and IT teams. Automated provisioning reduces human error, lowering the risk of security threats and non-compliance.

Along with automating the joiner/mover/leaver process, automation should also be leveraged for everything from workflows to reporting that helps maintain compliance.

AI/ML technologies can enhance how automation is used in these administrative processes, as well as in how identity tooling identifies risky anomalies for rapid incident response. Organizations that have AI-driven IAM tooling reported improved identity security in many areas.

AI/ML can also support analysis of historical data to help predict the outcome of proposed actions. Recommendations based on AI/ML enable reviewers to make faster, more accurate access decisions and focus on the high-risk access that most urgently requires attention.

## Methodology & Firmographics

*SailPoint commissioned Dark Reading to conduct a survey to explore identity and access management (IAM), identity-related breaches, and how organizations are automating identity management and developing policies around entitlements and authorization.*

*The survey collected data from 108 cybersecurity and IT professionals at organizations with 500 or more employees. Fielding was conducted online from January to March 2025. Respondents were recruited via emailed invitations containing an embedded link to the survey, which were sent to a select group of Dark Reading's qualified database.*

*The survey queried respondents with high-level cybersecurity and IT job titles, including cybersecurity and IT executive-level titles such as CISO (8%), CIO/CTO (8%), and chief risk officer (2%). Other titles included director/manager of security operations (14%), IT director/manager (19%), and VP of cybersecurity (6%). Other IT, cybersecurity, and business titles make up the remainder of the respondent base.*

*Twenty percent worked at companies with 500 to 999 employees, 40% at companies with 1,000 to 4,999 employees, 17% between 5,000 and 9,999, 11% between 10,000 and 49,999, and 12% at the largest-sized companies with 50,000 or more employees. Respondents worked at organizations representing more than 19 vertical industries, including banking and financial services, technology manufacturing, healthcare/pharma, education, and government, to name those cited by 6% or more.*

*Dark Reading was responsible for all survey administration, data collection, and data analysis. These procedures were carried out in strict accordance with standard market research practices and existing U.S. privacy laws.*