Delinea

2025 Identity Security Risks and Trends Report

Why CISOs Must Prioritize a Strong Identity Security Strategy—and Where to Start

Executive Summary

Strong identity and access management (IAM) combined with a modern identity security strategy is the foundation of any organization's overall security posture. Every transaction made, every document shared, every connection executed between cloud and on-premise resources, and every login requires robust authentication, authorization, and governance to uphold trust and ensure accountability.

This is no new revelation to chief information security officers (CISOs) and other cybersecurity leaders. However, in 2025, the challenges of ensuring the principle of least privilege and maintaining strong identity management have become far more complex than anyone could have imagined even just a few years ago.

In this report, we cover some of the most important trends that are driving identity security today. This examination extends far beyond looking at the outlook of traditional IAM products and solutions, and delves into strategies for authorization, entitlements, governance, privileged access management (PAM), and more. This analysis draws on a survey of 300 U.S. technology and security leaders, focusing on their identity-related strategies. It explored spending habits, key challenges, and future plans, and was further enriched by critical insights into recent identity threat trends provided by our internal research team.

Key takeaways:

- Identity security is a strong pillar of technology investments today, with most organizations spending 20% or more of their IT budget on identity and access management technology and processes.
- Identity security spending is on the rise, with 78% expecting to increase their budgets in the next year.
- Many organizations are maturing beyond a singular focus on strong authentication, with many organizations planning to invest in cloud infrastructure entitlements management (CIEM), identity governance and administration (IGA), and PAM in the coming year.
- Detecting and responding to identity threats is the number one priority for organizations as identity-focused vulnerabilities and attacks rise.

Read on to find out what this means for security and risk programs, and how CISOs and other leaders should use these insights to shape their identity security strategies in the coming year.

Identity is at the forefront of technology and business investments

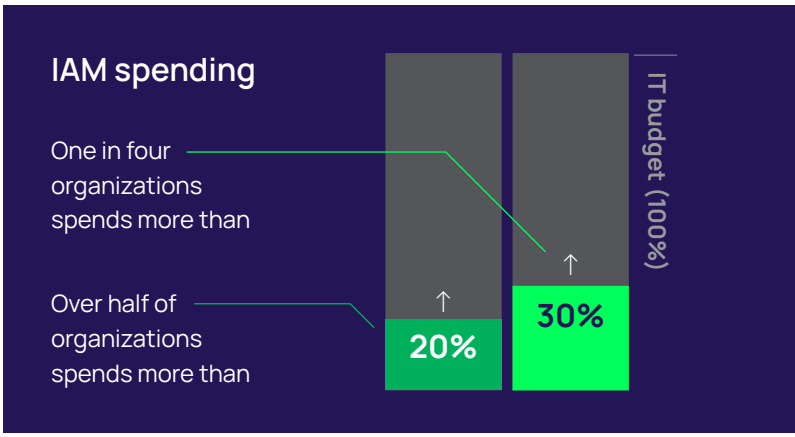
We started the survey by asking respondents about their budget plans and investment strategies around identity, both now and in the future. The results showed that identity management and identity security play a significant role in broader technology investments.

Over half of organizations dedicate more than 20% of their IT budget to IAM spending today, with one in four spending over 30%. At first, this may seem like a significant amount of budget dedicated to identity. However, it's justified by the critical role that identity management plays in managing and safeguarding complex relationships in modern digital ecosystems—encompassing humans, machines, bots, and AI models essential to business operations.

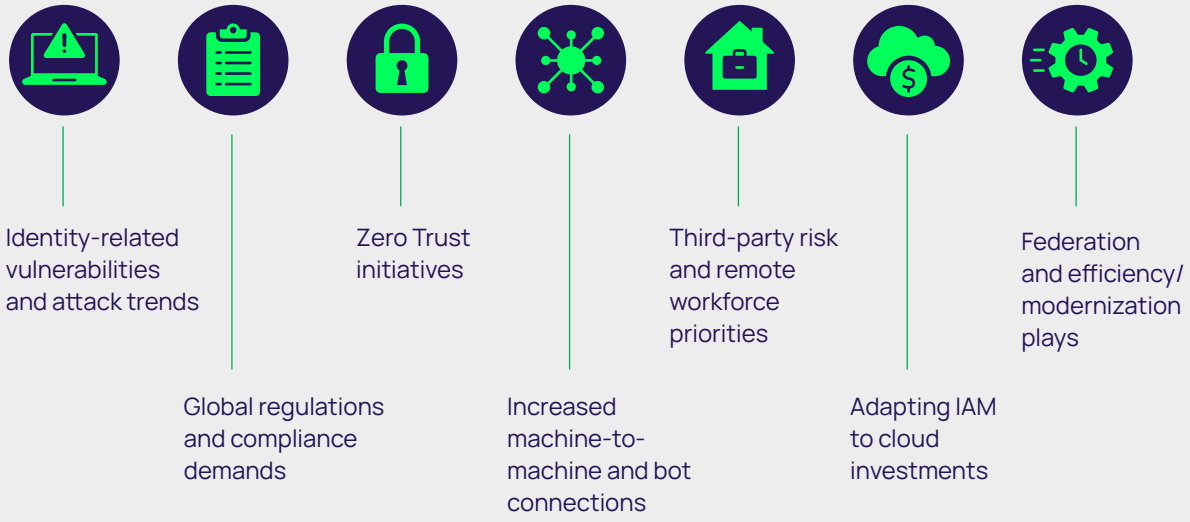
Most organizations recognize that these relationships will only grow more complex, requiring greater efforts in identity management as digital transformation continues to accelerate. In fact, 78% of those surveyed expect to increase their identity and access management budgets in the next year. And almost one in three said their budget will increase significantly. They'll need these investments to keep pace with the growing number of new systems being integrated into their infrastructure, driven by digital transformation initiatives, hybrid work environments, and the rapid adoption of cloud-based applications. As organizations expand their technological ecosystems, managing and securing access to these systems becomes increasingly complex, necessitating robust solutions to prevent unauthorized access, ensure compliance, and mitigate evolving cyber threats.

We believe identity is becoming a foundational part of digital transformation budgets, driven by the growing adoption of cloud and multi-cloud environments, as multifactor authentication (MFA) and single sign-on (SSO) have become table stakes for new deployments.

In addition, advanced organizations recognize that they need to make bigger investments to help appropriately assign entitlements, authorization, and to monitor activity based on who—or what—has access to a system or data store at any given point in time.



We speculate that some of the major drivers for increased identity spending include:

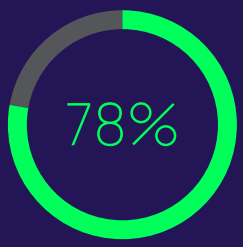


Ultimately, as organizations broadly modernize their technology infrastructure, they're also likely spending more to pay down technical debt. They're updating legacy identity architectures to account for new systems, new internal and external connections between on-premise and cloud ecosystems, and new threats targeting identity weaknesses that are emerging each day.

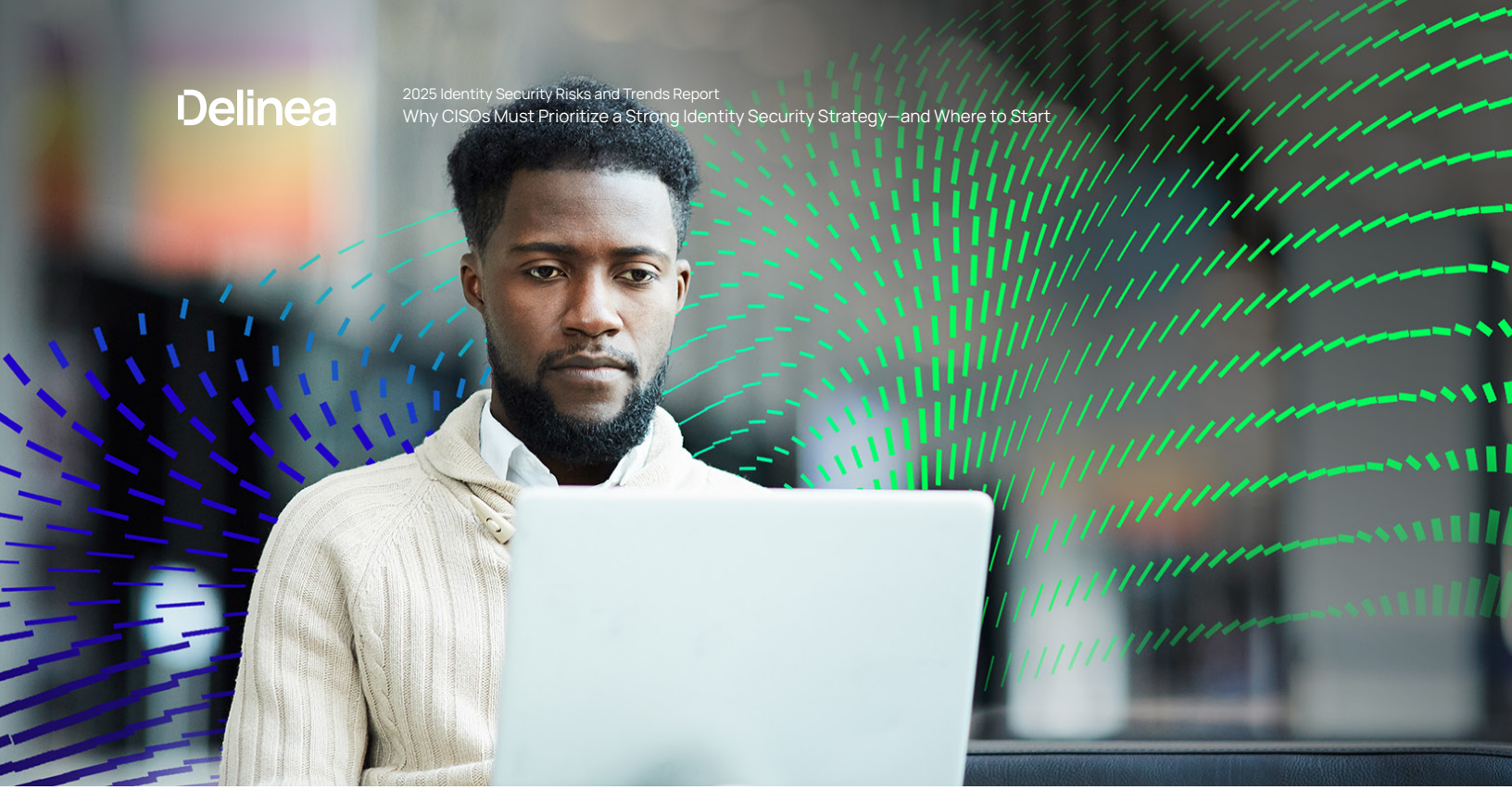
The role that identity security plays in anchoring cybersecurity goals in the coming year is also likely driving increased spending. When we asked respondents how high or low of a priority identities, related access, and entitlements are within their security program, 78% reported that they are of high importance. By digging specifically into the highest priorities around their IAM activity, security played a large role.

The top five priorities reported by those surveyed were:

1. Detecting and responding to identity threats
2. Securing credentials, secrets, and privileged accounts
3. Managing identities and entitlements in the cloud
4. Visibility into all identities and levels of access
5. Securing remote work and third-party risk



reported that priority identities, related access, and entitlements are of high importance within their security program



Tackling today's identity complexities

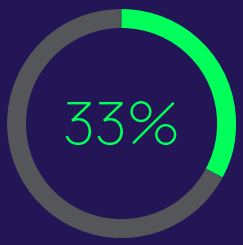
It's evident that substantial resources are now being directed toward identity investments. But how effective are these investments in truly reducing risk and maintaining visibility into identity activity? And how efficient is this spending?

As we dive deeper into the survey results and the technology trends our experts have observed in recent years, there are signs that organizations are overspending on duplicative and isolated identity technologies that fail to integrate seamlessly. And in many cases, while there's overlap in some areas, significant gaps remain.

The data reveals that unfocused and siloed spending often results in IAM infrastructure becoming a complex tangle of technical stacks, making it difficult and costly to manage. When asked about the biggest identity obstacles they face, complexity of existing infrastructure is far and away the biggest stumbling block, named by 33% of respondents.

The other obstacles are also tied to complexity. For example, in the second spot, resistance from users and stakeholders, which was named by 16%, is often a product of login friction and caused by convoluted and overly complex architectures.

It's tough for many to plan a way out of that complexity trap. Buyers encounter a proliferation of security vendors, a range of identity technologies, and a collection of identity-related definitions by analysts that's overwhelming for even the savviest cybersecurity practitioner or leader. And many organizations don't have enough of those savvy practitioners or the right technology foundation to start modernizing their infrastructure. Insufficient technology and a lack of skilled personnel were tied for the third biggest challenge, a troubling predicament given that both are essential to streamlining identity architectures.



of respondents named complexity of existing infrastructure as the biggest stumbling block

Nevertheless, after years of digital transformation projects that require deploying many different types of SaaS applications and cloud infrastructure, enterprises have been left facing the reality of what this means for identity. They're striving to streamline how they manage not just sign-in mechanisms but also how they govern the process and workflows of granting and denying authorization. For many, this will require smart consolidation and platform integration to create a streamlined path forward.

The survey revealed that the vast majority—88% of organizations—are considering consolidating vendors to streamline their IAM strategy, most of them within the next year. As organizations consolidate, they must balance the quest for IAM simplicity with the need to bolster IAM capabilities to match the broader complexity of IT systems. Simply consolidating at the expense of reducing identity security functionality is not a viable option, given the trends identity buyers must navigate. These trends include:

Trends identity buyers must navigate

- **Integration support:**
  Organizations need to support identity authorization and authentication for a lot of the connectivity in the 'background.' This includes a growing number of API connections between internal and external integrated apps.

- **Machine-to-machine connections:**
  The proliferation of machine-to-machine accounts is adding another layer of complexity for organizations. These connections between automated systems, AI platforms, DevOps environments, and other digital infrastructures are constantly in flux. They're becoming even more complex with the added layer of smart building and IoT connections. This is likely why our study shows that 28% consider securing non-human or machine identities a top priority for the coming year.

- **A wide range of human users and roles:**
  Aside from the variety of nonhuman identities, businesses also must contend with a wide range of human users and roles that need different levels of access. Not only are there employees in different departments and at different levels, but also there are contractors, temporary employees, business partners, visitors, supply chain stakeholders, third-party vendors, and more. They all need differing levels of entitlements to systems and the complexity on this front is driving investments in identity governance in order to coordinate authorization.

Finally, it's important to note that it isn't just large enterprises that are contending with these complexity issues. The complexity problem is greatly impacting small to midsize companies because they don't have the resources or the skill sets to handle the evolving challenges.

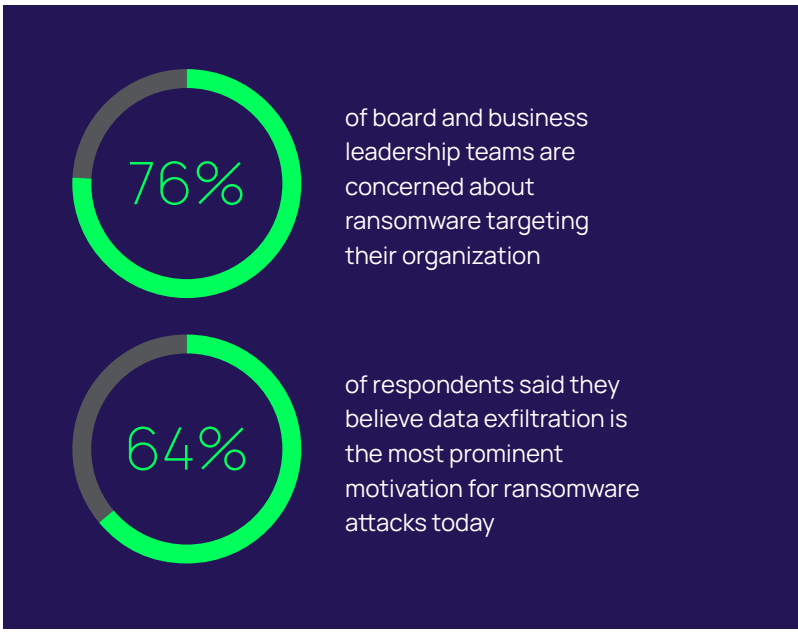
Examining the top priority: Detecting and responding to identity threats

As we explained above, half of survey respondents said detecting and responding to identity threats was their top priority around IAM. Clearly, security leaders are concerned with the range of different attacks that are fueled by identity-related vulnerabilities and misconfigurations—and for good reason. These attacks often fuel further identity-related attacks when attackers gain unauthorized access to sensitive systems and steal usernames and passwords to other sensitive systems and privileged accounts.

Take, for instance, the threat of ransomware. Previous Delinea research shows that well over half of organizations have been impacted by ransomware in the past year and 76% of board and business leadership teams are concerned about ransomware targeting their organization. Many of these attacks are executed using stolen passwords from phishing, privilege escalation—especially when targeting sensitive systems for which organizations are most likely to pay a ransom—and other identity-focused techniques.

The better bad actors get at gaining unauthorized access to more sensitive systems, the more money they're making from their extortion schemes. Recent industry research shows that the average ransom payment increased by 500% in 2024 as attackers focused on gaining access to critical infrastructure, medical technology, and other highly sensitive systems.

But there's more risk to ransomware than just asking for the ransom. Ransomware attacks are caused by identity insecurity but they're also causing further identity-related attacks down the road as bad actors double-dip on their attacks by exfiltrating data—including sensitive credentials once they're in a system they hold hostage.



While precise figures are difficult to pin down, the general consensus is that the majority of ransomware income still comes from ransom payments. However, the sale of stolen data represents a growing and highly profitable aspect of ransomware operations, particularly for groups employing double extortion tactics. Data sales may provide an additional revenue stream that boosts overall earnings. In an earlier ransomware survey by Delinea, 64% of respondents said they believe data exfiltration is the most prominent motivation for ransomware attacks today.

Delinea researchers have been analyzing data to track the volume of attacks potentially contributing to the dark web's growing pool of stolen credentials. Last year, 4,257 websites were held ransom—an average of 355 attacks per month. These breaches not only disrupt organizations but also provide a foundation for escalating identity-related threats and attacks in the future.

Identity-related CVEs and significant attacks in 2024

In spite of identity attack trends around ransomware and other threat activity, most organizations express confidence in their ability to detect and respond to identity threats. However, vulnerability and attack data from across the industry suggest this confidence may be misplaced. Leaders are generally confident in what they are aware of and in the systems they've deployed so far. However, the greatest risks often stem from systems they're unaware of or have overlooked securing.

Our analysis of industry trends reveals that attackers have a wealth of opportunities to exploit weak identity components in software and cloud infrastructure. For example, identity-related Common Vulnerabilities and Exposures (CVEs) accounted for nearly 13% of all CVEs reported in the past year. This is especially concerning because these vulnerabilities often serve as gateways for initial access and enable lateral movement within compromised environments. Even seemingly minor flaws can have severe consequences when combined with other vulnerabilities.

To address these risks, technologies like identity threat detection and response (ITDR) and credential vaulting are becoming critical investments. If an identity system is breached, ITDR can help detect and respond to the intrusion. This is an essential capability, even if it's not applicable to every vulnerability. Similarly, vaulting technologies play a key role in securing credentials and limiting the breach blast radius should an attack occur.

As the IAM landscape consolidates, organizations face an additional challenge: their identity products themselves becoming potential threat vectors. While consolidation offers efficiency, it also concentrates risk, creating tempting "one-stop shopping" opportunities for attackers. This underscores the need for robust defensive strategies to protect against evolving threats.

CVEs		2024
Month	**Total CVEs**	**Identity-related CVEs**
January	1,142	117
February	1,759	229
March	2,640	396
April	3,239	407
May	3,386	409
June	2,752	424
July	2,894	295
August	2,708	361
September	2,420	336
October	3,322	383
	26,262	3,357

Significant identity-related cyberattacks from 2024

Needless to say, savvy cyber criminals are following these identity threats and using them to their advantage. The past year saw a series of identity-related cyberattacks, as criminals leverage identity flaws in security postures.

Delinea researchers identified some of the most impactful among these, each of which offer a glimpse into the different approaches attackers are using to steal credentials and strengthen their ability to gain unauthorized access to systems and data:

MC2 data

A significant cybersecurity breach at MC2 Data, a U.S.-based background check firm, resulted in the exposure of 2.2TB of personal information, affecting approximately 106 million Americans. This unprotected database has made sensitive data, including names, email addresses, phone numbers, dates of birth, and home addresses publicly accessible. With third of the U.S. population's background information now compromised, the risk of identity theft has surged, potentially leading to financial fraud, unauthorized access to personal accounts, and long-term privacy issues for the affected individuals.

Ivanti VPN compromise

This attack exploited vulnerabilities in Ivanti's VPN software, which is widely used by various organizations, including U.S. government agencies. The attackers were able to infiltrate the networks of multiple agencies, potentially accessing sensitive government data. This incident highlighted the critical need for robust security measures in VPN infrastructure to protect against such sophisticated attacks.

Microsoft executive accounts breach

High-profile Microsoft executive accounts were compromised in a targeted attack. The breach involved sophisticated phishing techniques and possibly other methods to bypass security measures. The attackers gained access to sensitive information, which could have far-reaching implications for Microsoft's operations and security posture.

Snowflake data-theft attacks

Customers of Snowflake, a cloud-based data warehousing company, experienced widespread data theft. The attackers exploited vulnerabilities in Snowflake's platform to access and steal data from multiple customers. This incident underscored the importance of securing cloud-based services, and the potential risks associated with data warehousing solutions.

Okta breach

In October 2023, Okta, a major identity and access management company, confirmed that hackers had accessed data on all of its customers. The attackers used a stolen credential to infiltrate Okta's support case management system. Initially, Okta reported that around 1% of its customers were affected, but later it was revealed that the breach impacted all of its customers. Consequently, the industry continued to see fallout in 2024 unfold from this major breach. The attackers stole customer-uploaded session tokens, which could be used to break into the networks of Okta customers. The stolen data included full names, email addresses, phone numbers, usernames, and details of some employee roles. This breach has raised concerns about the security of identity management systems and the potential for further phishing or social engineering attacks targeting Okta customers.

Maturing beyond the MFA fixation

For a long time, many organizations have conflated IAM with MFA and SSO. Traditionally, technologists have thought of IAM with a capital "I" and lowercase "am" as the focus has been on authentication rather than authorization and identification. We're starting to witness a sea change in that paradigm, however.

Our survey asked about deployment trends and unsurprisingly, MFA was noted as the most commonly used technology for securing and managing identities. It was tied with CIEM or cloud security posture management (CSPM), and both were cited by 57% of respondents. This was closely followed by identity threat detection and response (ITDR), which is currently used at just under half of organizations.

The mix looked similar when we asked respondents what they expected to most heavily invest in over the coming year. The most commonly cited technology was once again MFA, which was named by 51% of those surveyed. CIEM/CSPM closely followed, named by 49%. Interestingly, though, IGA was tied for second, also at 49%. ITDR and privileged access management (PAM) rounded out the top five, named by 46% and 43%, respectively.

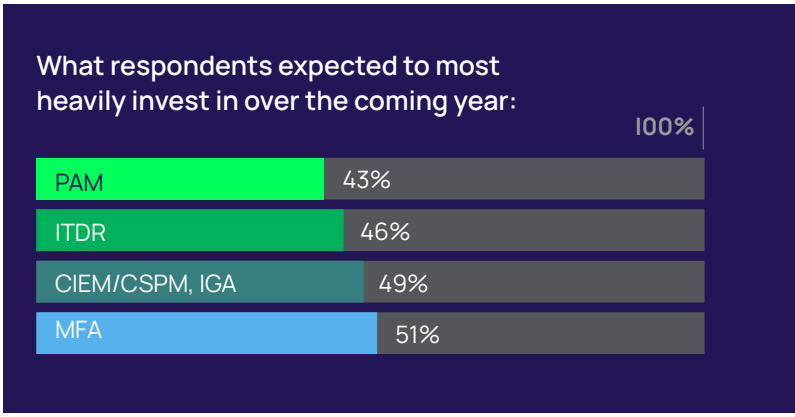
This points to what our technologists and security experts have been seeing in the field: Maturing organizations have taken the first and easiest steps to investing in identity and they're slowly dipping their toes into more formidable waters.

At this point, most organizations have mastered authentication for their most critical applications. MFA is typically used in some way, and most organizations continue to invest in broadening its adoption across more use cases and more users while maturing the way they use and administer it. Simultaneously, cloud adoption trends and the aforementioned digital transformation use cases have been gaining momentum. As previously mentioned, 43% of organizations say that managing identities and entitlements in the cloud is a top priority. That's why CIEM/CSPM has been such a draw. Many organizations are tackling authorization, figuring out how to most efficiently handle entitlements, managing just-in-time access, and generally driving their identity strategy to better adhere to the principle of least privilege.

Newer technologies like CIEM and ITDR are likely the shiniest items on the investment list. They haven't been available for long and it's likely that many organizations invest in these solutions through their identity provider as an easy-to-add-on option that's relatively simpler to adopt.

The increasing emphasis on IGA and PAM reflects a shift toward more complex solutions that demand significant administrative and planning efforts for successful deployment. These systems often require foundational work, such as policy development and entitlement approval, which relies on extensive cross-functional collaboration and strong top-down support. Momentum is growing—our top priority list reveals that 45% of respondents identified securing credentials, secrets, and privileged accounts as a key focus for the coming year.

The focus on PAM, which is primarily an authorization play, indicates that organizations are starting to mature beyond their MFA fixation. At the end of the day, this is going to ensure that IAM focuses as much on how data is accessed as it does on authenticating the identity of the account used to do so.



How AI is shaping the future of IAM

Given this push to deepen IAM investments to better mature authorization, governance, and identity threat detection, tech leaders are looking for ways to accelerate the way they tackle these tougher identity security problems with artificial intelligence (AI). We asked organizations when, or if, their organization plans to adopt AI-driven identity technologies and the vast majority—over 94%—have something in the works either now or in the near future. A clear 55% have already adopted or are already in the process of adopting AI-driven technology, while 23% are currently evaluating AI-driven tech. Additionally, 16% say it's planned for 2025.

We believe that AI fits hand-in-hand with future strategies to improve identification and authorization, and will help speed up detection and response to identity threats. Based on emerging trends, we anticipate AI will play an increasingly significant role in:

- Tying asset inventory and classification with identity strategies.
- Powering more granular identity-tied monitoring for HR and corporate investigative purposes.
- Helping identity governance teams reduce policy and access sprawl and more efficiently manage accounts and entitlements.
- Driving better detection of identity behavioral anomalies and using that data to contextualize security operations data.

Additionally, many organizations are likely to start looking toward identity strategies to help them protect broader AI infrastructure across the business. Our experts believe that in 2025, many organizations will be seeking ways to use identity security to protect AI systems, AI agents, LLMs, training models, and access to AI models.

The blueprint for building an identity security strategy

This report offers some important cues to security leadership about the spending and prioritization tendencies of their peers. As you're planning your own roadmap for 2025, your identity security strategy should be a top priority. Here are some of the key considerations as you make a plan.

Don't lose sight of the importance of authorization

Strong authentication is now table stakes for secure technology infrastructure. But it is only one part of the identity security puzzle. Managing entitlements and automating authorization is what will truly make it difficult for attackers to successfully access sensitive systems and data. Our survey showed that CISOs and other cybersecurity leaders increasingly understand that this will be the security game-changer in the coming years.

Continuous discovery is crucial

The growing list of machine-to-machine accounts, different types of user roles, and connections between on-premise, cloud, and hybrid environments creates a daunting complexity issue as it is. But what really makes it difficult to identify and keep tabs on who and what needs to be authorized and authenticated is the fact that the accounts and the access levels are constantly changing. Your inventory and ability to keep tabs on identities needs to be real-time and constantly evolving with the dynamic nature of access in modern digital ecosystems.

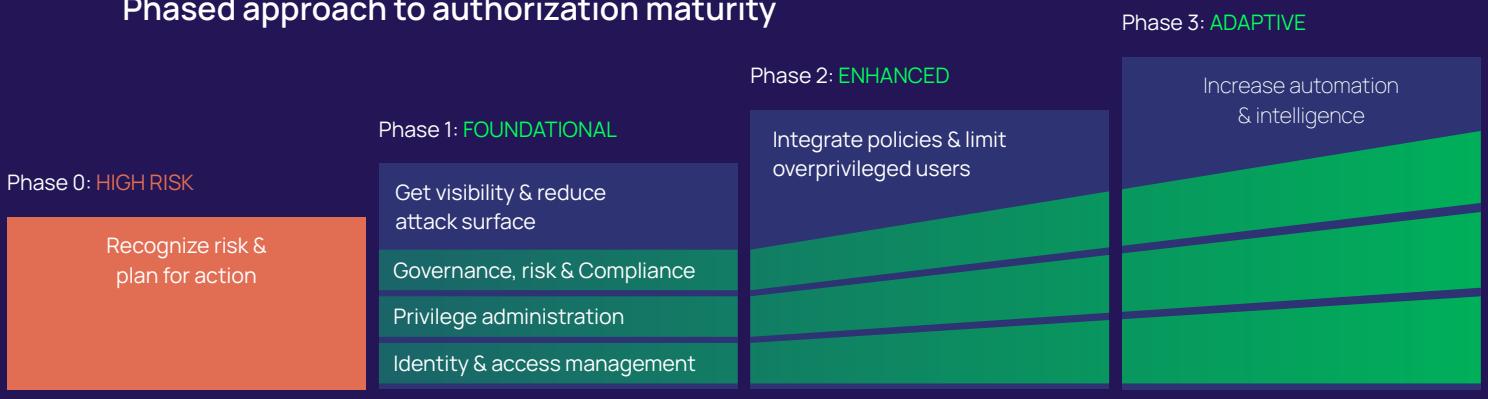
Lean on platform integration

Platformization makes it possible to consolidate without losing key identity security functionality or extensibility as threat or infrastructure trends call for added identity capabilities. A platform that allows for broad interoperability enables adding functions that will still be integrated with unified management as you mature. Platforms that lean on identity as a service (IaaS) and platform as a service (PaaS) can offer resources needed for management and support, putting more sophisticated identity security strategies in the realm of possibility for smaller businesses.

Take a phased approach

The reason so many organizations have spent more time on authentication than they have on identification and authorization is because authorization maturity is hard to achieve. It can feel daunting to pull together all of the elements an organization needs to discover credentials, monitor access, integrate policies, and eventually increase the use of automation to manage conditional access. This can only be achieved through a phased crawl, walk, run approach. Phase one is the foundational stage of getting visibility and reducing the attack surface. Phase two is integrating policies and limiting over-privileged users. Phase three is increasing automation and intelligence.

Phased approach to authorization maturity



- No/limited visibility
- Manual employee join, move, leave
- Credentials manually managed
- Full admin rights

- Discover & vault IDP, CSP, ERP credentials
- Enforce MFA for admin access
- Detect account takeover threats
- Establish privileged remote access
- Monitor critical business apps
- Automate user identity lifecycle

- Discover & vault all credentials
- Clean up admin accounts
- Enforce temporary least privilege
- Enforce MFA for system & app login
- Enforce MFA for privilege elevation
- Risk analytics for access request workflows
- Certify entitlements for critical apps

- Automate app identity lifecycle
- Enrich SOC with identity threat intel
- Manage service account lifecycle
- Risk scoring for enhanced conditional access
- Leverage audit data & ML analytics to detect and respond to threats
- Automate identity threat remediation

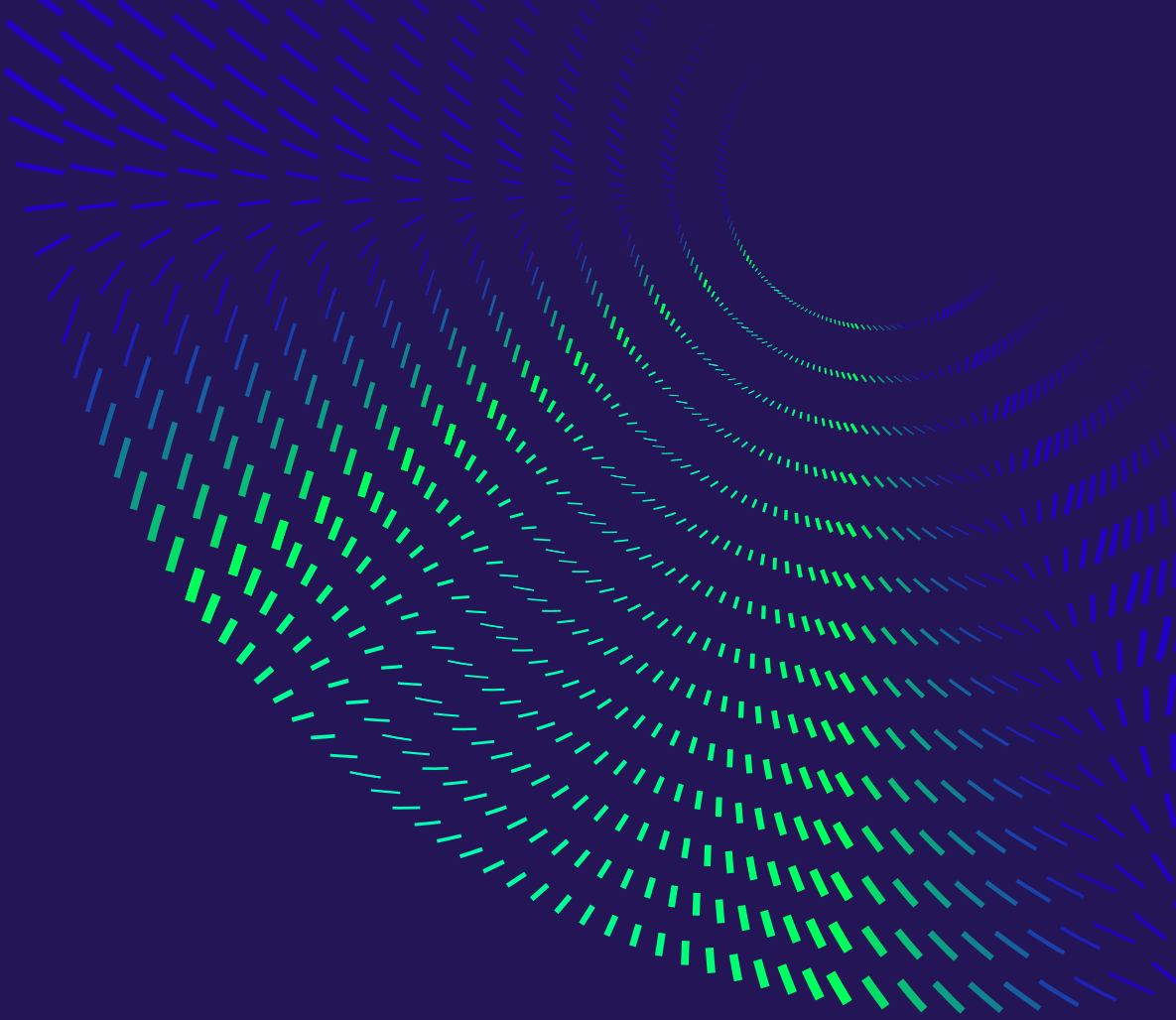
Uplevel SOC capabilities with ITDR

Identity threats are a huge concern for cybersecurity today and organizations need monitoring purpose-fit to identify identity threats. As security programs seek to reduce dwell time and the impact of compromised identities, ITDR can be a huge boon. As leaders look at their options for ITDR and how that fits into their security operations center's technical stack, they should ask their practitioners what the organization does to detect identity threats in the context of account takeover or lateral movement within identity systems.

Simultaneously streamline and mature your identity security capabilities

CISOs and other cybersecurity leaders will have to keep the momentum going for identity security in 2025. As organizations wrestle with complex cloud-based ecosystems and evolving threats, simply throwing money at the IAM budget will not be enough. Leaders must find a way to streamline their identity platforms and deployments while also maturing their capabilities around authorization and the detection of identity threats. This will take a robust strategy and sound architectural planning to carry out.

To learn more about how Delinea can help you crawl, walk, and run your way toward greater identity security maturity, check out delinea.com/products/identity-lifecycle-management



Delinea

Securing identities at every interaction

Delinea is a pioneer in securing identities through centralized authorization, making organizations more secure by seamlessly governing their interactions across modern enterprise. It applies context and intelligence throughout the identity lifecycle, covering cloud and traditional infrastructure, data, and SaaS applications to eliminate identity-related threats. Delinea uniquely provides intelligent authorization for all identities, allowing precise user identification, appropriate access assignment, interaction monitoring, and swift response to irregularities. The Delinea Platform accelerates adoption and boosts productivity, deploying in weeks, not months, requiring just 10% of the resources compared to competitors. Discover more about Delinea on Delinea.com, LinkedIn, X, and YouTube.

SISS-WP-0125-EN