SPECTEROPS
Creators of BloodHound

Trends in Identity Attack Path Management 2026

Agentic AI raises the stakes for identity security

APRIL 2026

In collaboration with Omdia

Executive summary

Organizations are investing more in technology to manage a growing identity attack surface. Across large enterprises, identity security is drawing more budget, attack path visibility is rising on the strategic agenda, and identity Attack Path Management (APM) is moving from early interest into broader adoption.

Adoption alone does not create durable outcomes, however. Many organizations are still working through the people, process, and governance changes needed to operationalize identity APM and turn visibility into measurable, repeatable risk reduction. That tension runs through this year's research: the market has advanced, while practice maturity remains uneven.

> **This report examines how security and identity leaders are prioritizing, adopting, and operationalizing Identity APM, how AI and non-human identities are raising the stakes, where operational hurdles persist, and why maturity looks different depending on organizational structure and industry context.**

Survey composition

For this report, SpecterOps commissioned Omdia to survey 541 cybersecurity decision-makers at organizations with 10,000 or more employees across the United States, Canada, the United Kingdom, France, Germany, and Australia. **Respondents held decision-making responsibility or influence over cybersecurity strategy, identity and access management, directory services, system procurement, or related areas.**

The respondent base skews toward large enterprises and highly regulated sectors. Nearly half of respondents work at organizations with 10,000 to 24,999 employees, and the most represented industries are banking, financial services and insurance, energy and utilities, and healthcare. Respondents come from both IT and cybersecurity functions, with representation across Director, Vice President, and C-level roles.

541
Cybersecurity decision-makers

6
Regions (US, Canada, UK, France, Germany, Australia)

10K+
Employees per company

BFSI, healthcare, energy/utilities
Top industries

IT & cybersecurity
Functions

Director, VP, C-level
Seniority

PART 1

Identity APM is becoming a core part of identity security

Identity risk is becoming a mainstream security priority. The survey indicates that organizations are increasingly treating attack path management as an important part of identity security. Spending is rising, attack path visibility is high on the priority list, and a meaningful share of organizations have already moved from evaluation into deployment.

Identity security investment is rising quickly

Identity security is attracting increased investment, signaling broader recognition that identity risk needs dedicated attention. In 2026, 75% of respondents report increased identity security spending compared with the prior year. **That is higher than the shares reported for the other security technology categories tested, including data security, SecOps, OT/IoT, and infrastructure.**

Budget movement is often a stronger signal than stated interest alone. It suggests that identity risk is earning real prioritization inside enterprise security planning. The 18% jump in respondents who say their organization has increased identity security spending (75%, up from 57% in 2025) may well be due to the growing identity security challenge surrounding agentic AI and non-human identities.

According to research from Entro Labs,[1] 97% of NHIs have excessive privileges, and over 5.5% of AWS NHIs are full administrators ("Super NHIs"), with some organizations reaching as high as 18%.

1. lp.entro.security/2025-state-of-nhi-and-secrets-in-cyber

Attack path visibility is becoming a top-tier security priority

Organizations increasingly view visibility into attack paths and privilege relationships as a strategic need. When asked about top cybersecurity priorities over the next 12 months, 46% of respondents selected enhancing visibility into attack paths and privilege relationships. That places it ahead of integrating generative AI and agentic AI solutions for the business, which was selected by 43%.

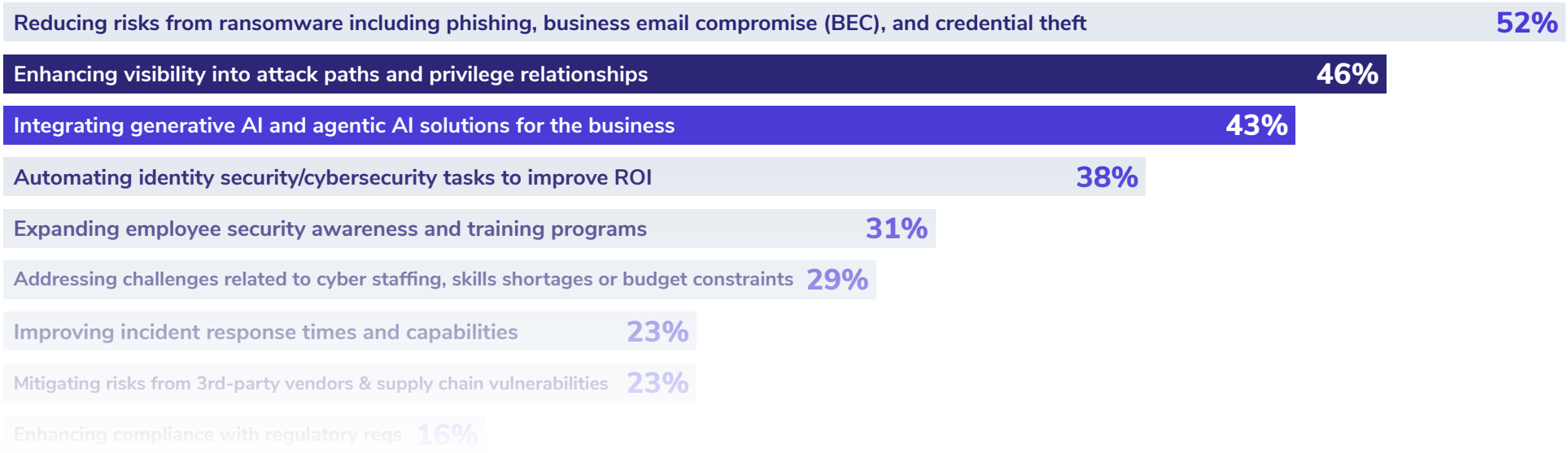
The same survey also shows that identity risk remains prominent in how organizations think about current and future threats. Taken together, those results suggest that **identity-related exposure is staying near the center of enterprise security thinking.**

Identity APM has moved beyond experimentation

Identity APM is no longer confined to early adopters. In this year's survey, 35% of respondents say they have fully implemented an identity-based APM solution, up from 21% in 2025. Another 30% say they are actively researching or evaluating options. More than half, 54%, report using automated attack path discovery with APM tools to examine identity-based attack paths.

> These numbers point to a market that has moved past awareness. Some organizations are already operating with Identity APM in place, while many others are building the business case, running evaluations, or integrating the capability into broader security programs.

What are your organization's top cybersecurity priorities over the next 12 months?

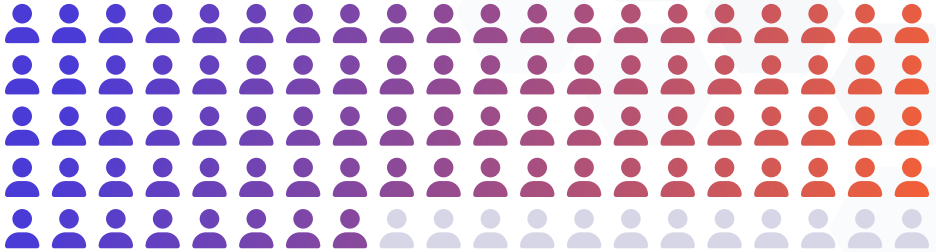


PART 2

AI and NHIs raise the stakes

AI is increasing the urgency of identity security. According to a November 2025 report from McKinsey,[2] "sixty-two percent of survey respondents say their organizations are at least experimenting with AI agents." Recent survey research from Omdia reflects this shift.

According to its Cybersecurity Decision Maker Survey, some 88% of identity security respondents were either already using or planning to use AI agents in the next 12 to 18 months.



As organizations adopt agentic AI and autonomous workflows, they are also expanding the number of non-human identities, credentials, and trust relationships they must govern. The survey suggests that this shift is sharpening focus on visibility, access relationships, and the operational demands of managing identity risk at greater scale.

AI is accelerating identity complexity and raising the stakes for APM

As organizations adopt agentic AI and autonomous workflows, they are also increasing the number of non-human identities, credentials, and trust relationships they must govern. In that context, the survey suggests that identity security and attack-path visibility are becoming more urgent. Respondents rank attack path visibility and privilege relationships at 46% ahead of AI integration at 43% as a near-term priority.

> **They also rank security for AI/genAI and identity security as the top two areas where they are seeking more innovation from technology partners.**

2. mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

It's not a surprise that AI security and identity security are nearly matched in terms of priority. As enterprises face increasing board-level pressure to adopt agentic AI, the number of non-human identities will continue to proliferate, and the relationships between human and non-human identities will grow by orders of magnitude. As a result, **AI and agentic AI security are intrinsically linked to identity security**. AI increases the pressure to understand how access can chain together, how privileges propagate, and how identity-related exposure can be controlled before it becomes operational risk.

Non-human identities are already part of the challenge set

Non-human identities are already showing up in how organizations describe identity-risk challenges. In the survey, respondents identify managing non-human identities as one of the key challenges they face in governing identity risk.

This matters because non-human identities often expand faster than the governance structures designed to manage them. As service accounts, automation bots, workload identities, and AI-driven workflows become more embedded in enterprise operations, security teams face a larger and more complex identity graph. **Understanding how privilege chains together human and non-human actors will become more important as that environment grows.**

Why AI raises the stakes for Identity APM

AI agents and automated workflows expand machine identities and access relationships. More autonomy creates more trust propagation, more credentials, and more ways for access to chain together across systems. In that context, **the need to discover, prioritize, remediate, and continuously reassess attack paths becomes more urgent.**

The survey does not prove that AI is already the dominant driver of identity risk, but it strongly suggests that organizations building operational maturity in Identity APM will be better positioned to manage the next phase of identity complexity.

PART 3

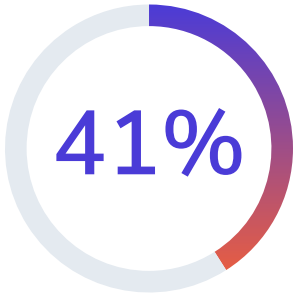
Technology adoption is ahead of operational maturity

Enterprises increasingly recognize the value of attack path management. The harder work lies in building a practice around it. The survey shows organizations setting concrete program goals, adopting risk-based remediation approaches, and increasing evaluation cadence. It also reveals that operational friction remains.

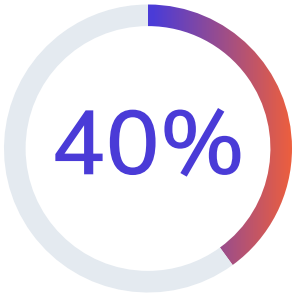
Program goals show a shift from visibility toward risk reduction

Organizations are focusing on outcomes that extend beyond discovery. When asked about their overall APM goals over the next 12 months, respondents most often cite:

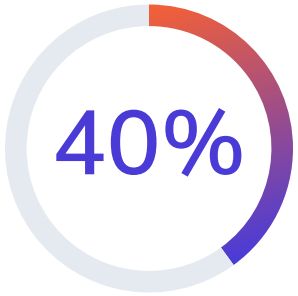
Reducing the number of critical or exploitable attack paths:



Improving visibility among identity relationships and in relation to Tier Zero or critical resources:



Enhancing automated detection and remediation capabilities:



These goals suggest that many programs are evolving from baseline visibility into more structured risk reduction efforts. Visibility still matters, but organizations are also concentrating on what happens after attack paths are identified.

Prioritization sits at the center of operationalization

65%
prioritize by risk score or impact assessment once attack paths have been identified.

Risk-based prioritization is emerging as a central part of Identity APM practice. Once attack paths and misconfigurations have been identified, the most common reported remediation process is to prioritize by risk score or impact assessment at 65%. Many organizations also report using automated tools for remediation at 58% and assigning issues to relevant teams for manual remediation at 57%.

Prioritization is also the most frequently cited implementation challenge at 41%. That tells an important story: organizations are building toward a risk-based operating model, while many still struggle with the volume, complexity, and workflow pressure that come with deciding what to address first.

Operational gaps persist even in deployed programs

Implementation does not automatically translate into mature practice. Among respondents who have implemented an identity-based APM solution, the most frequently cited solution gaps are:

Better prioritization of risks and remediation actions	56%
Automated remediation capabilities	56%
Integration with existing security tools	47%
Real-time attack path detection	45%

Integration with existing security tools is in the top three. This finding clarifies what deployment does and does not accomplish. The technology can establish visibility and help teams start to organize around attack paths. It does not, by itself, resolve the operational demands of triage, workflow integration, hybrid coverage, and sustained remediation.

Continuous evaluation is becoming a marker of maturing programs

Organizations are increasingly treating Identity APM as an ongoing practice rather than a one-time assessment. Among respondents who have implemented an APM solution, continuous evaluation of attack paths rises materially year over year, with the strongest gains appearing in high-frequency evaluation, especially continuous monitoring.

That shift points to a more durable operating model. Rather than approaching attack path management as a periodic hygiene exercise, more organizations appear to be building a continuous cycle of discovery, prioritization, remediation, and reassessment.

From tool adoption to practice maturity

The survey suggests that many organizations are moving beyond initial tool adoption and beginning to operationalize Identity APM through prioritization, remediation, and more continuous evaluation.

For readers interested in a deeper framework for benchmarking practice maturity across people, process, and technology, see the:

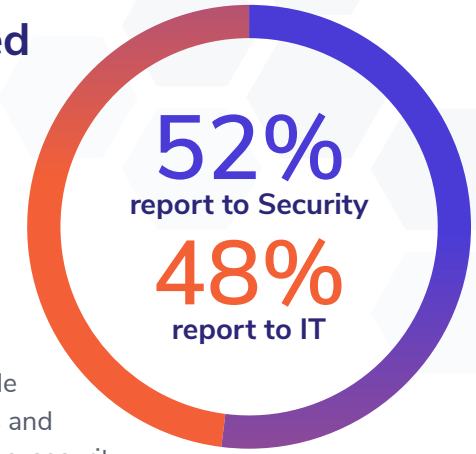
SpecterOps Identity APM Maturity Model ›

PART 4

There is no single maturity curve

Organizations are not all operationalizing Identity APM in the same way. Practice maturity varies based on ownership model, industry requirements, and the shape of the environment being protected.

Identity APM is shaped by operating model, not just tools



How organizations organize identity work influences how they operationalize APM. In the survey, identity management reports almost evenly to Security at 52% and IT at 48%. Responsibility also spans multiple functions, including IAM, IT operations and infrastructure, cloud security or DevOps, security operations, compliance and governance, and outsourced providers.

Identity APM sits at the intersection of identity, infrastructure, and security operations. In many enterprises, no single team fully owns the underlying problem. **That makes coordination, prioritization, and remediation as important as the technology itself.**

Who is primarily responsible for identity management at your organization?

Identity and access management team	50%
IT operations/infrastructure team	41%
Cloud security or DevOps team	41%
Security operations team	39%
Compliance & governance team	30%
Outsourced to a third party	28%

Industries are moving along different pathways

The survey does not support a simplistic ranking of industries from least to most mature. It does suggest that organizations are progressing along different operational pathways.

BFSI shows stronger signals on cadence and assessment rigor. It has higher continuous evaluation rates than healthcare and energy/utilities, along with stronger use of pen testing and red teaming and greater emphasis on support for hybrid environments.

Healthcare stands out for its emphasis on practical decision support, especially risk prioritization and step-by-step remediation plans. Energy and utilities show more pressure around scalability and integration-related needs and gaps.

> **These differences matter because they show how maturity can take different forms. In some sectors, it expresses itself through cadence and formalization. In others, it appears in remediation guidance, scalability requirements, or integration pressure.**

Industry pathways toward Identity APM maturity

The survey points to distinct patterns across industries:

BFSI

Stronger signals on cadence, formalization, and hybrid support

Healthcare

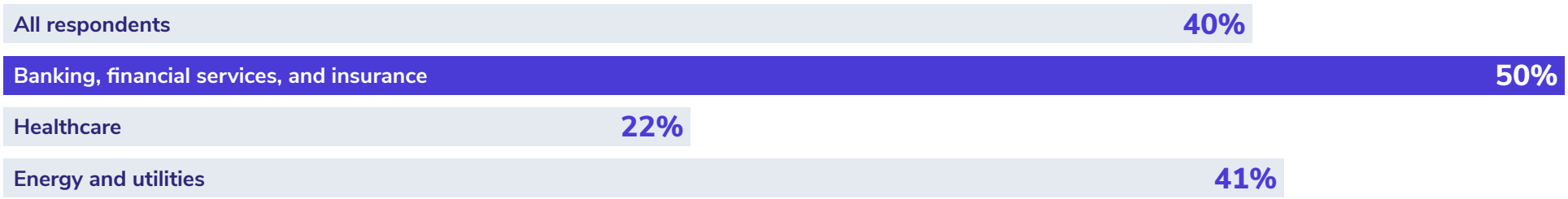
Stronger emphasis on prioritization and remediation guidance

Energy and utilities

Stronger pressure around scalability, integration, and execution complexity

In what capacity does your organization evaluate attack path management in your identity environments?

Continuously:



Conclusion

Identity APM adoption has moved beyond experimentation. Spending is rising, attack path visibility is a strategic priority, and many organizations have already implemented or are actively evaluating APM solutions.

AI and NHIs add urgency to that trend. As machine identities, credentials, and trust relationships expand, organizations will need stronger ways to understand how access can chain together and where privilege creates exposure.

The next chapter is operational maturity. The organizations that gain the most value from Identity APM will be the ones that turn visibility into prioritization, remediation, and continuous evaluation through stronger workflows, ownership, and governance.

> **That process will not look identical across sectors, but the direction is clear: the market is moving from interest in Identity APM toward the harder work of building it into practice.**