

TRENDS IN IDENTITY & ACCESS MANAGEMENT:

Automation to AI

With workforces now overwhelmingly hybrid and the added complexity of field and fully remote workers, this expanding identity landscape dramatically increases the number of provisioning events, access policies, and risk vectors (including AI-driven entities) that organizations must manage.

Although organizations have broadly adopted modern Identity and Access Management (IAM) platforms, Gatepoint Research conducted a survey to identify where execution gaps persist, particularly in lifecycle automation, internal identity management, and governance at scale. Sixty-seven IT and cybersecurity leaders participated, including C-level executives (12%), vice presidents (21%), directors (52%), and senior or department managers (15%), reflecting both strategic leadership perspectives and hands-on management experience.

Participants represented a mix of large enterprises (46% with \$1.5B+ in annual revenue) and mid-sized organizations in identity-critical sectors:

25%
Financial Services and Insurance

25%
Technology and Telecom

22%
Consumer, Retail, Media and Business Services

15%
Industrial and Manufacturing

13%
Healthcare and Life Sciences

Business Case Priorities to Automate, Scale or Otherwise Improve

Role-defined, attribute-driven provisional access

55%

HR-driven lifecycle(HRIS as source of truth)

34%

Automate time-based access privileges

24%

Granular multi-app provisioning and actions

19%

Centralize risk signals for automated response and control

15%

Distill and share critical provisioning/de-provisioning information

9%

License optimization for SaaS apps

9%

Automate conflicts/errors during the provisioning process

7%

Issues That Led to Prioritizing These Cases

61%

Complex IT infrastructure

30%

External identity access

30%

Inefficient process for on/off-boarding and role changes

27%

Limited resources

21%

Evolving compliance requirements

19%

Elevated security risk

18%

Audit findings/ evidence collection burden

12%

Shadow IT

6%

Shared passwords

3%

Scaling up or down

How AI Agents/Non-Human Identities Will Influence Workforce IAM Strategy

55%

Expand identity governance to cover machine + service accounts

51%

Require automated lifecycle management for agent accounts

42%

Heighten need to manage secrets, credentials, + service account sprawl

39%

Drive tighter visibility + monitoring of agent-to-app activity for compliance + risk

37%

Increase in demand for granular, time-limited access policies

34%

Extend role-based models to include AI-driven tasks

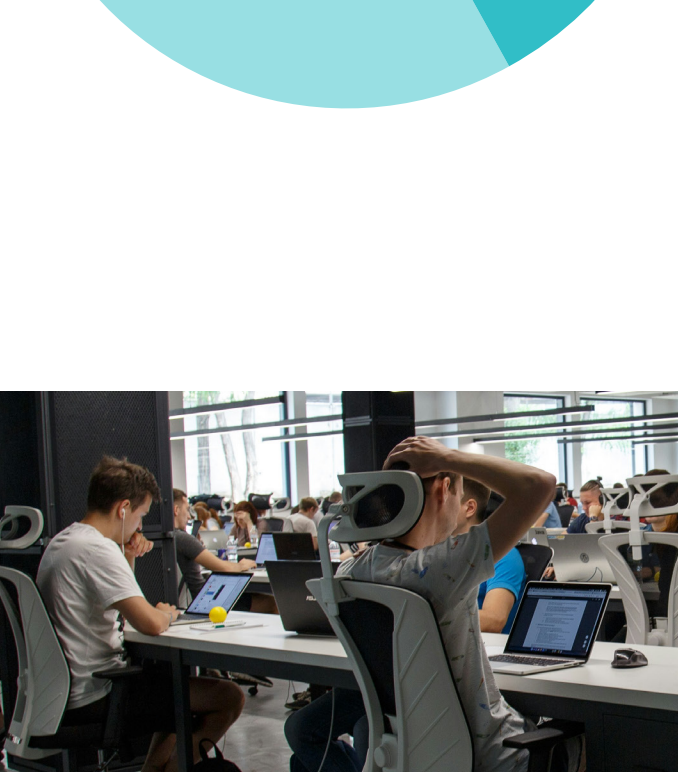
33%

Introduce new governance requirements for contractor/ partner + AI collaboration

12%

Have minimal or no impact on workforce IAM strategy

Benefit That Would Prompt Investment in Better IAM Technology



- Greater risk reduction
- Increased efficiency/usability
- Reduced help desk tickets/ faster IT throughput
- Tighter compliance
- Better scalability
- Improved reporting/analytics and executive dashboards
- Faster audit readiness

Research conducted by:



Research sponsored by:



About Okta

Okta is an identity and access management company that provides cloud-based software to help organizations manage and secure user authentication across modern applications. It also enables developers to build identity controls into applications, web services, and devices.

Okta secures every identity—from human users to machine and AI-driven entities.

[Discover more at okta.com.](https://www.okta.com)

[Learn More](#)