

Securing the Identity Perimeter with Defense in Depth

Organizations continue to rely on user and machine identities that are susceptible to compromise, misuse, and theft. Modern, cloud-managed identity services are available, but organizations have been slow to pivot their security programs to an approach that focuses on identity orchestration and experiences. ESG surveyed IT and cybersecurity professionals responsible for identity and access management programs and solutions to gain insights into these trends.

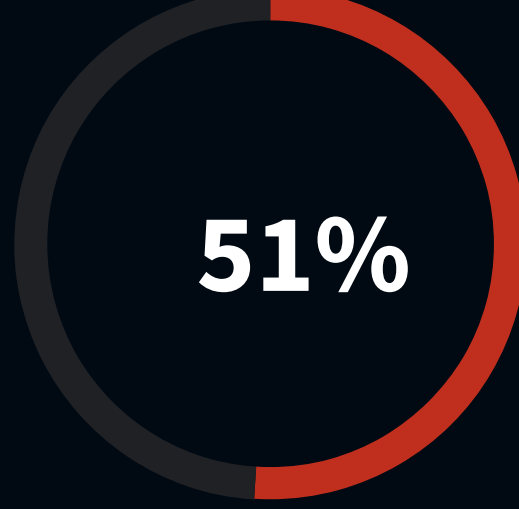
Identity Management Is Complex

Complexity of IAM leads to extensive use of third-party services.

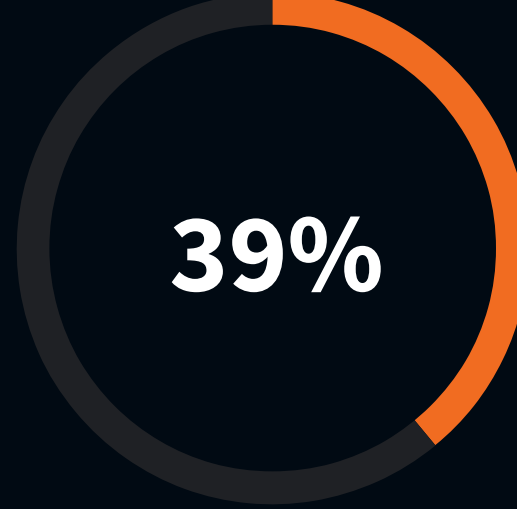
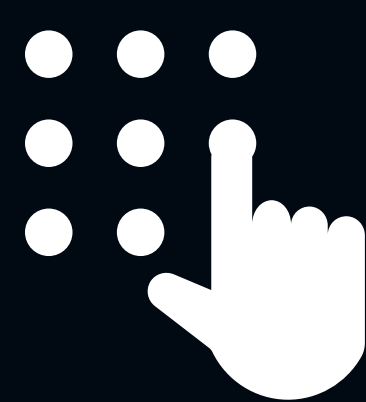


87%

of organizations use third-party identity and access management (IAM) services.



PAM is among the top three solutions/controls for my organization



PAM is among the top five solutions/controls for my organization

40%

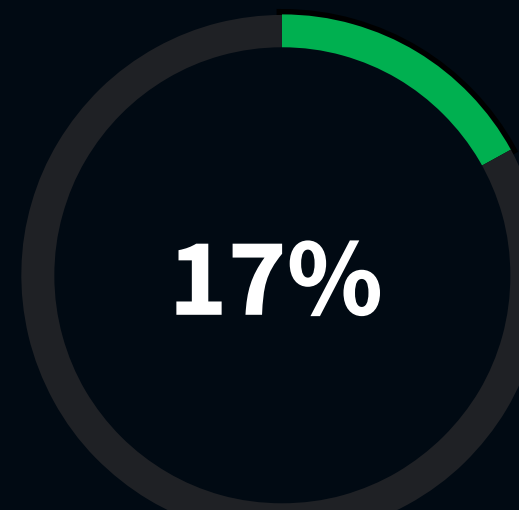
expect PAM to increase security without creating user friction.

The Need to Operationalize Different Forms of Authentication

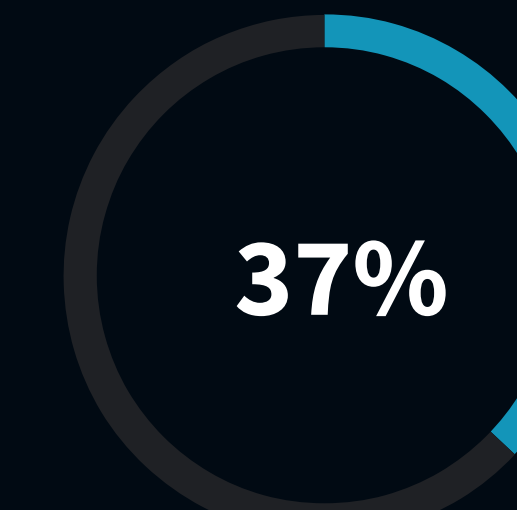


58% currently use multi-factor authentication.

Passwordless is becoming strategic.



We have started to selectively eliminate passwords



We are actively evaluating/testing eliminating passwords

Majority of organizations use SSO.



55%

of organizations currently use SSO technology.

48%

expect SSO to reduce friction and improve the user experience.

Assessing Risk across Human and Non-human Identities Is a Priority

Percentage of organizations that have suffered a breach due to:



46%

Identity-related threats



36%

Permission-related threats



37%

Workload/deployment model-related threats

Identity Proofing, Screening, and Monitoring Reduce Risk

Top 3 risk screening processes currently used.



78%

Background screening for new employees or third parties



77%

Verifying certifications/accreditations for positions such as lawyers/law/state bar; doctors/medical (MD); registered nurses, finance and accounting (CPA), educators/teachers, etc.



68%

Criminal screening and fingerprinting

Likelihood of multiple identity records for a single employee or customer.

Extremely likely for employees

61%



Extremely likely for customers

52%



Most common identity proofing/verification use case.



Verifying identity attributes with authorized sources and identity validity confirmation

72%

Identity Market Dynamics

Identity security budget change.

Increase slightly,
47%



Increase significantly,
37%

Nearly a third of organizations expect new IAM spending to be focused on CIEM and/or CIAM.

[LEARN MORE](#)

For more from this ESG research study, including guidance for organizations that want to detect and prevent identity-driven attacks, read the ESG research report, *Securing the Identity Perimeter with Defense in Depth*.