CISCO DUO

Navigating the Identity Security Terrain in 2025:

Challenges and Strategies in a Digitally Transformative Era

As digital transformation continues to reshape industries, the complexity and importance of robust identity access management (IAM) practices have surged to the forefront of cybersecurity strategies.

In an era marked by AI-driven threats and sophisticated phishing attacks, Cisco's survey reveals glaring gaps in the security posture of many organizations.

Duo commissioned independent research firm TrendCandy to survey 650 Security and Data Ops leaders in a multinational study that finds identity is the new security.

The margin of error for this study is +/- 3.8% at the 95% confidence level.

Security Left Out of Identity Decisions

TO DO: Embed security reviews into every identity-related decision.

74%

of IT leaders admit identity security is often an afterthought in infrastructure planning.

Privileged Access, Poor Visibility

WHY THIS MATTERS: Privileged accounts are high-value targets; invisibility increases risk.

55%

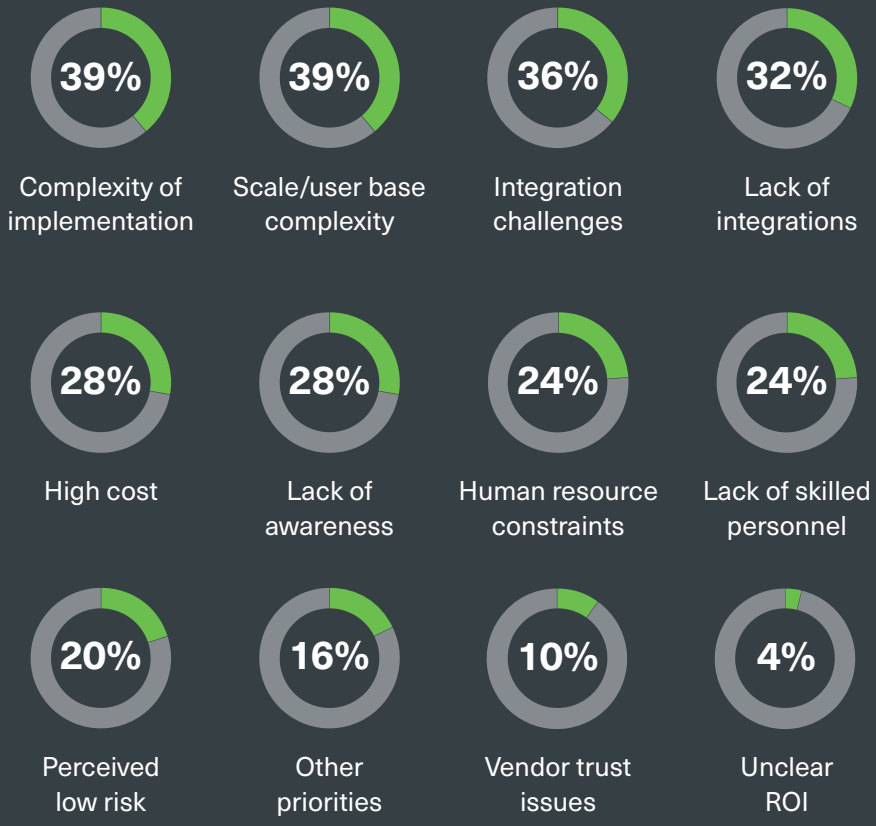
of teams lack full visibility into admin and privileged user access.

Identity Sprawl is Real

Identities are stored in an average of 4.8 systems per organization, from IDPs to HRIS.

WHY THIS MATTERS: Dispersed identity data hampers unified security enforcement.

Top Barriers to ITDR Adoption

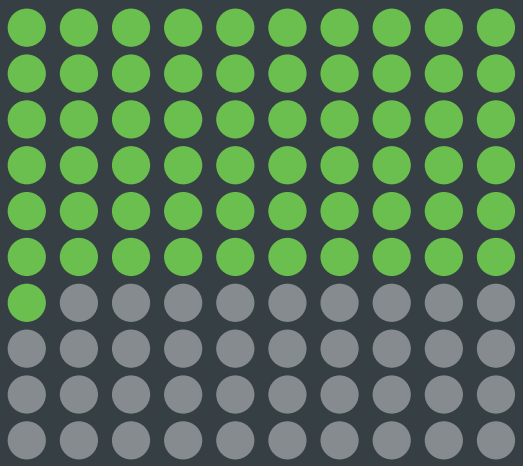


KEY INSIGHT: Technical and operational complexity outweighs financial barriers in ITDR deployment.

Passwordless Ambitions Meet Friction

61%

want to move to passwordless access but expect deployment challenges.



KEY INSIGHT: The future is passwordless, but retrofitting legacy systems is the delay.

Third-Party Access a Major Worry

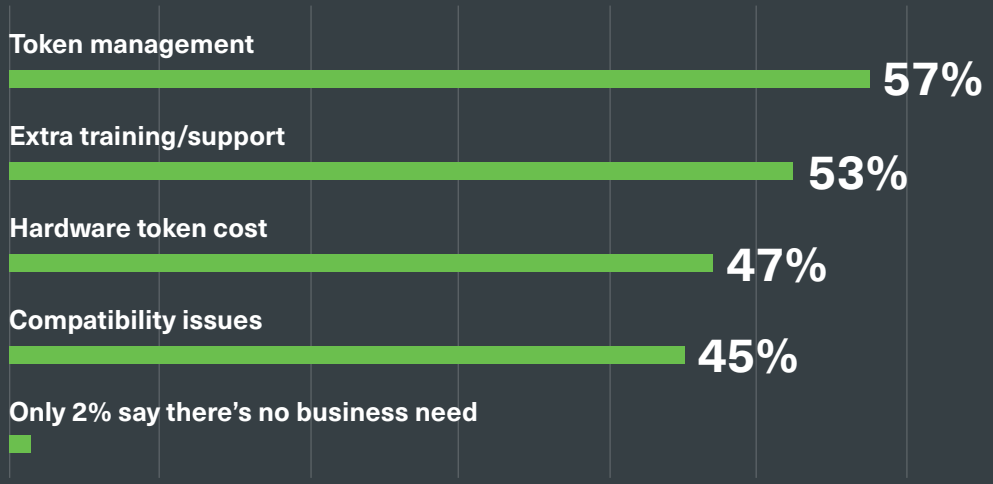
86%

of IT leaders are concerned about inadequate controls for contractors and third-party access.

TO DO: Deploy tailored access and monitoring solutions for external identities.

Biggest Phishing Resistance Hurdles

KEY INSIGHT: Resistance stems from operational burdens, not lack of demand.



Phishing-Resistant MFA a Top Priority

WHY THIS MATTERS: Password-based methods no longer meet evolving threat levels.

87%

believe phishing-resistant MFA is critical to their security strategy.

MFA Still Incomplete

69%

are worried that MFA isn't deployed across all devices and apps.

WHY THIS MATTERS: Incomplete MFA coverage is a critical risk vector.

Device Hygiene: Recognized but Unreliable

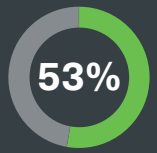
While 79% agree device hygiene is vital, only 26% are highly confident in universal device security.

TO DO: Establish continuous endpoint monitoring and hygiene enforcement.

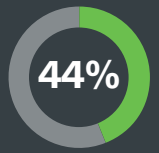
Identity Issue Resolution is Fragmented

IT teams navigate 5 tools on average to resolve a single identity-related issue.

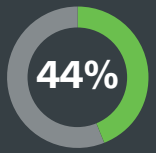
Why Consolidate Identity Tools?



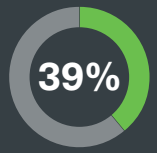
Better user experience



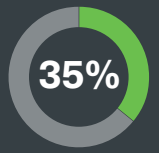
Easier compliance



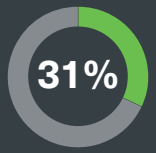
Stronger security posture



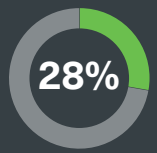
Lower ops cost:



Reduced identity sprawl



Increased automation



Reduced complexity

Better threat detection

Simpler management

KEY INSIGHT: Identity consolidation is about strategic simplification, not just savings.

Vendor Consolidation Gaining Momentum

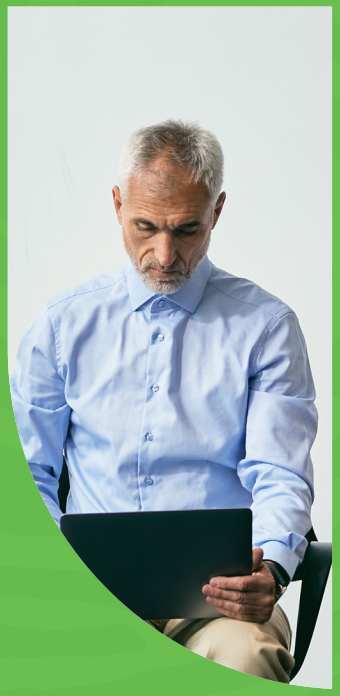
79%

of teams are actively exploring vendor consolidation to improve identity security visibility.

KEY INSIGHT: Tool sprawl is driving a pivot to fewer, more comprehensive platforms.

CISCO

DUO



Contact Sales

Free Trial

duo.com