CISCO DUO

Challenges and Strategies from IT and Security Leaders

Highlights from the 2025 State of Identity Security Report

In a world where AI-driven threats and sophisticated phishing attacks are reshaping cybersecurity, strong identity and access management (IAM) is no longer optional—it's essential.

Cisco Duo's 2025 State of Identity Security report surveyed 650 Security and IT leaders across North America and Europe to uncover the stark realities and hidden vulnerabilities of today's identity security postures. The research reveals why identity is the new security and highlights the urgent need for organizations to rethink their strategies.

Explore these insights to stay ahead of evolving threats and build a resilient, future-proof identity security framework.

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

Confidence in Identity Providers is Worryingly Low

Despite the foundational role identity providers (IdPs) play in access control, confidence in their ability to stop identity-based attacks remains strikingly low.

WHY THIS MATTERS: A lack of confidence is heightened by complex identity systems and concerns about limited visibility into potential weaknesses.

Only a third

(33%) of leaders are confident their current identity provider (IdP) protects against identity-based attacks.

Leaders acknowledge the vital role of identity security and are increasing budgets.

51%

of organizations have suffered financial losses due to identity-related breaches.

82%

of financial decision-makers have increased budgets for identity security.

AI-driven attacks are accelerating identity security growth and system modernization

AI-driven phishing, insider threats, and supply chain attacks top the list.

85%

of companies are adopting security-first identity practices to counter AI-driven threats

Identity Security Comes Too Late

WHY THIS MATTERS: Modern identity solutions must have security functionality by default, not as an expensive add-on.

74%

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

Identity Sprawl is Real

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

Dispersed identity data hampers unified security enforcement.

Identity Issue Resolution is Fragmented

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

Phishing-Resistant MFA a Top Priority

WHY THIS MATTERS: Traditional 2FA methods like SMS and email no longer meet evolving threat levels.

87%

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

Only 19% **have deployed FIDO2 tokens.**

Often, these hardware tokens are reserved for privileged users.

Biggest Phishing Resistance Hurdles

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

Passwordless Ambitions Meet Friction

61% want to move to passwordless access but expect deployment challenges.

Leaders agree Identity Security delivers ROI

- Faster Incident Response: **51%**
- Smoother User Logins: **43%**
- Higher Compliance Audit Success: **37%**

Get the full report.

CISCO DUO

Redefining — and restoring — trust in identity.

Speak with an Expert | Free Trial | **duo.com**