CISCO
DUO

2025 State of Identity Security:

Challenges and Strategies from IT and Security Leaders

New Cisco Duo survey finds that 85% of companies are adopting security-first identity practices to counter AI-driven threats.

Introduction

The increasing adoption of remote work, cloud-first operations, and distributed supply chain networks has rapidly evolved identity from a tactical IT consideration to a strategic pillar of cybersecurity. In a world where AI-driven threats and sophisticated phishing attacks are redefining security requirements, strong identity and access management (IAM) is no longer optional—it's essential.

Cisco Duo's latest study 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.

Highlights

Facing an Identity Crisis

Whether it's the challenge of managing identities across multiple systems or the strain of resolving issues with separate tools, the data highlights that disjointed processes and legacy infrastructure are holding organizations back. Only 33% of leaders are confident in the security their identity provider offers.

Phishing Resistance in a New Threat Era

AI-driven phishing, identity spoofing, and insider risks are changing how organizations view authentication and authorization. Amongst security professionals, 87% agree that phishing-resistant MFA is critical, but just 19% have fully implemented FIDO2 tokens. That's a major disconnect between awareness and execution.

A Need for Security-first Identity

Yet, the momentum is shifting. 82% of financial decision-makers are increasing identity security budgets and 85% are adopting security-first identity strategies to counter AI-driven threats.

From this eBook, get findings and actionable insights from other leaders and companies looking to modernize their identity security.

Survey Methodology

Duo surveyed 650 IT and security leaders across North America and Europe. The margin of error for this study is +/- 3.8% at the 95% confidence level.

What You Will Learn in this eBook

- Why identity infrastructure complexity and confidence are now the biggest barriers to effective security—and how simplification can improve posture and visibility
- The gap between the value placed on telemetry and its practical implementation, and what's needed to bridge it
- How identity sprawl, fragmented visibility, and legacy systems can create blind spots in identity infrastructure
- What's holding back broader adoption of phishing-resistant MFA, passwordless, and identity posture management—and how leaders are prioritizing progress despite these challenges
- How today's top identity threats, from AI-driven phishing to insider risks, are reshaping security investment and tool consolidation strategies

Who This eBook is For

- Chief Information Security Officers (CISOs)
- IT Directors and Infrastructure Leads
- Identity and Access Management Architects
- Compliance and Risk Officers
- Security Operations Center (SOC) Analysts

Facing Complexity and a Confidence Crisis

From legacy tool sprawl to device and posture visibility, leaders anticipate significant challenges as identity threats escalate and security gaps widen. Security-first Identity becomes a priority.

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.

33% of security leaders are confident their identity provider protects against identity-based attacks.

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

ISPM Tools Are Underutilized

Identity Security Posture Management (ISPM) offers a strategic framework for enforcing policy and improving security outcomes—but adoption is lagging.

32% believe they have a fully effective Identity Security Posture Management solution.

TO DO: Evaluate current ISPM capabilities against known frameworks and prioritize gap remediation. Regular identity security posture checks can help identify high-impact recommendations tailored to the organization.

74% admit security is an afterthought.

Explore what security-first identity and access management looks like for your organization.

Identity Security Often Comes Too Late

Security often enters the conversation after core infrastructure decisions have been made—creating persistent misalignment between architecture and risk mitigation.

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.

Telemetry is Valued but Incomplete

Nearly all security leaders understand the strategic importance of identity and device telemetry—but integration into daily operations is inconsistent.

TO DO: Invest in solutions that unify and operationalize telemetry data across platforms.

97%

value identity and device telemetry, but only 52% have it fully integrated.

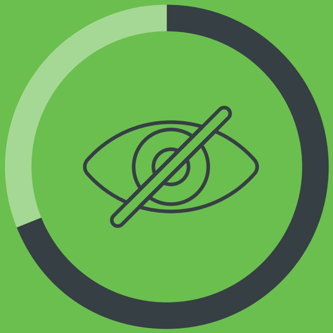
010111
0110100
101011

Visibility Into Identity is Fragmented

Lack of visibility into identity risk—especially privileged access and dormant accounts—remains a critical vulnerability.

69%

lack full visibility into identity vulnerabilities, and 55% into admin access.



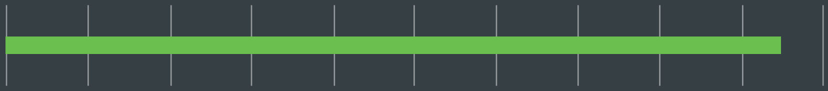
WHY THIS MATTERS: Unseen identities and privileged accounts are high-risk blind spots.

Complexity Is the Core Issue

From policy enforcement to incident response, identity-related complexity is undermining security fundamentals across the board.

94%

say complexity in identity infrastructure challenges security posture.



KEY INSIGHT: Simplification should be a top architectural goal.

With only 33% confident in their identity provider, can you risk standing still?

Modern identity providers should feel simple, secure, scalable. Learn how to manage identities from day one.

Identity Sprawl is Unchecked

The average enterprise identity is now spread across nearly five separate systems, introducing friction and increasing the attack surface.

Identities are stored in an average of

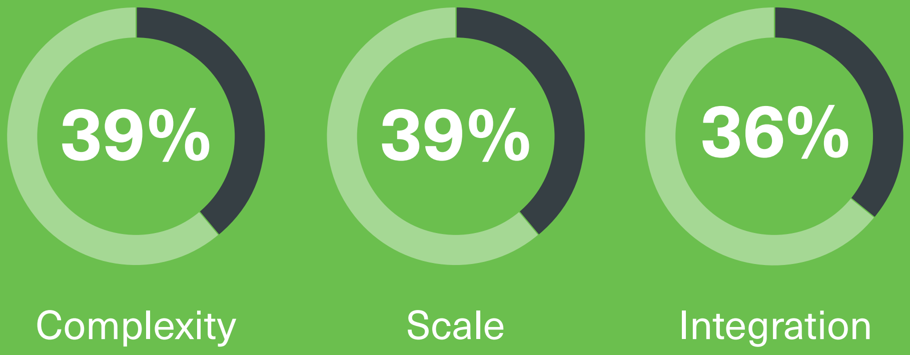
4.8 systems.

WHY THIS MATTERS: Dispersed identity data hampers unified security enforcement, and makes visibility across identity providers challenging.

ITDR Is Held Back by Deployment Friction

Identity Threat Detection & Response (ITDR) solutions are a rising priority, but complexity, scalability, and integration concerns are stalling rollout.

Top barriers include:



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

Persistent Phishing Threats & MFA Gaps

Advancing identity-based attacks drive a need for deployable end-to-end phishing resistance that doesn't compromise on usability.

MFA Gaps and Phishing Resistance

MFA Still Incomplete

Many organizations still lack full MFA coverage across devices and applications, creating persistent vulnerabilities.

69%

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

WHY THIS MATTERS: Gaps in MFA due to complex deployment, inconsistent coverage, and additional costs are a leading vectors of identity-based attack. Incomplete MFA coverage is a critical risk vector.

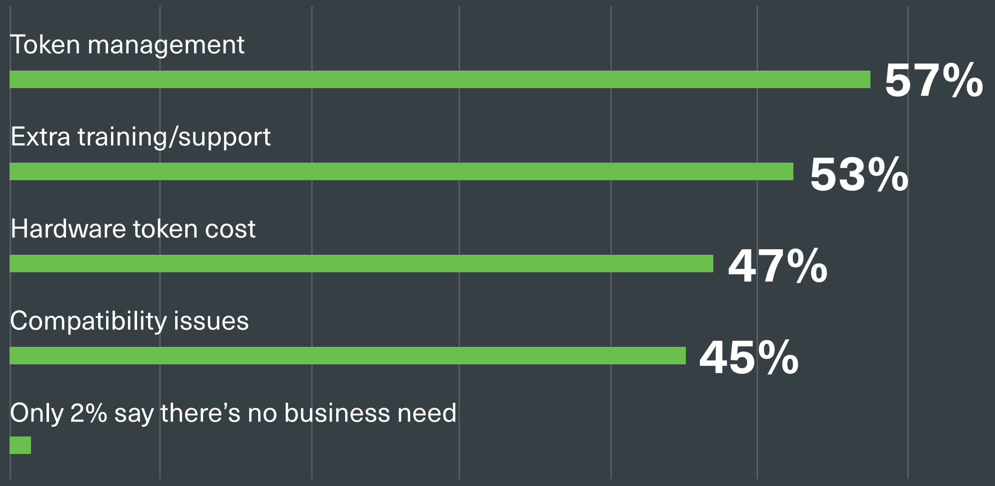
→ Stay ahead of credential-based attacks. See how to start the journey towards a passwordless future today.

The Biggest Phishing Resistance Hurdles

Leaders agree that phishing-resistant MFA is critical—but operational friction remains a major barrier to scale.

87%

prioritize phishing-resistant MFA, but only 30% feel confident in their phishing controls.



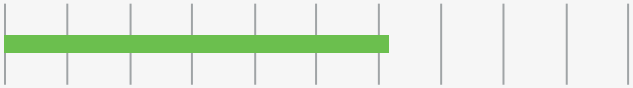
KEY INSIGHT: Resistance stems from operational burdens, not lack of demand.

Passwordless is a Goal, Not Yet a Reality

Despite clear support for passwordless access, legacy integration and workforce readiness remain major hurdles.

61%

want to move to passwordless access, but expect challenges.



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

FIDO2 Adoption is Low

Hardware tokens offer strong phishing resistance, yet full implementation of FIDO2 remains rare suggesting resource and prioritization gaps.

Only **19%**

of teams have fully implemented FIDO2 tokens.

TO DO: Assess hardware token fit for high-risk user groups. Evaluate phishing-resistant authentication methods that don’t require additional investments, like proximity-based verification.

Usability shouldn’t be a trade-off for security.

Eliminate login fatigue with a seamless access experience that doesn’t require extra hardware. Get phishing-resistant MFA that is easy to deploy.

A Need for Security-First IAM

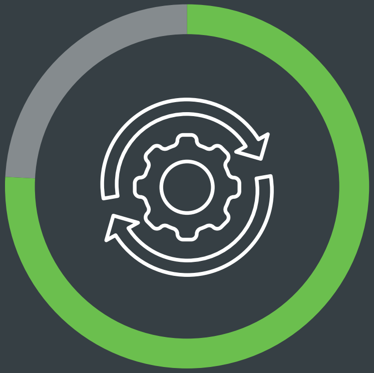
Treating security as an add-on can result in additional costs, complexity, and misalignment that decreases overall visibility. Modern IAM protects the expanded identity perimeter and prioritizes security from the start.

Integrated Solutions Are Essential

As multi-cloud adoption rises, tool interoperability has become non-negotiable for efficient and secure identity operations.

76%

say identity tools must integrate with AWS, Microsoft, and Google.



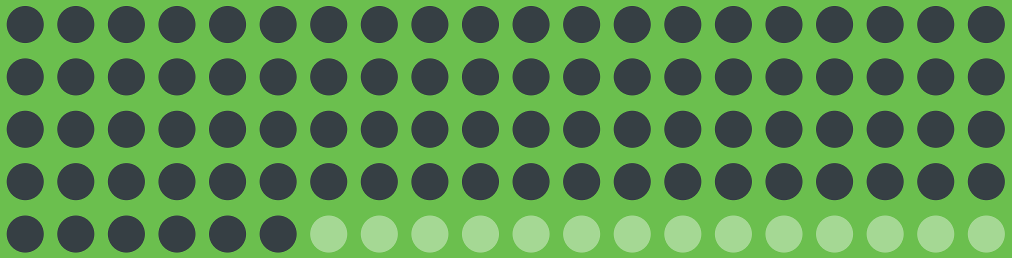
TO DO: Prioritize platform-agnostic or extensible solutions in procurement.

Third-Party and Insider Threats Are Growing

The perimeter has expanded—and most organizations are underprepared to manage access and risk from contractors and internal actors.

86%

are worried about inadequate contractor controls. 57% reported unauthorized access.

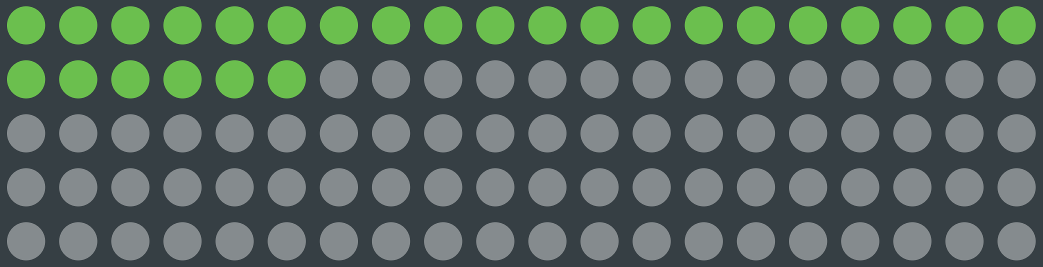


TO DO: Deploy tailored access and monitoring solutions for external identities. Consider storing third-party or temporary identities in a separate user directory that enables easy provisioning, deprovisioning, and granular access controls.

Device Hygiene Needs Improvement

Endpoint risk is a growing concern, especially as remote and hybrid work environments stretch traditional enforcement methods.

Only **26%** are highly confident in universal device security.



TO DO: Establish continuous endpoint monitoring and hygiene enforcement. Enforce security patches and get visibility into device health on all accessing devices—managed or unmanaged.

Top Identity Threats for 2025

Security leaders are preparing for a new wave of threats driven by AI, insider misuse, and increasingly sophisticated credential theft.

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

KEY INSIGHT: Threats are diversifying, but insider and AI threats dominate risk assessments.

Vendor Consolidation is Gaining Ground

Tool proliferation is creating operational drag—prompting leaders to explore identity vendor consolidation as a path to simplification and clarity.

79%

are exploring it to improve identity security visibility.

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

Security Investment is Rising

With budgets increasing, identity leaders have a critical window to accelerate modernization and close long-standing gaps.

82%

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

KEY INSIGHT: Security teams have momentum—now's the time to push forward critical initiatives.

Financial Impact of Identity Failures

The cost of identity breaches is no longer theoretical—more than half of surveyed organizations have suffered measurable financial damage.

51%

of organizations have suffered financial losses due to identity breaches.

WHY THIS MATTERS: Identity risk isn't theoretical—it hits the bottom line.

CISCO

DUO

Cisco Duo’s survey data paints a concerning picture of identity security readiness in 2025: complexity, fragmentation, and underutilized tools are exposing organizations to avoidable risks.

Yet with rising budget support and growing executive awareness, the opportunity is ripe for transformation. Organizations that adopt integrated, security-first IAM strategies stand to leap ahead in resilience and readiness. From passwordless ambitions to phishing-resistant MFA, the path is clear: secure identity is no longer optional—it’s mission-critical.

→ **Take our Identity Self Assessment to see how your organization compares to its peers**

Speak with an Expert

Free Trial

duo.com