Survey Report

The State of Identity:

How organizations are bridging the confidence gap

ID dataweb | CIO DIVE

Custom content for ID Dataweb from Studio by Informa TechTarget

Identity has moved to the front line

Identity-based attacks are well known. Paradoxically, many organizations feel unprepared for them.

Credential abuse remains the top initial access vector for intruders. Why break in when you can log in? This reality should challenge assumptions about where the security perimeter begins and ends. But does it really?

Impersonation, social engineering, and credential abuse now underpin the majority of successful breaches. Traditional perimeter controls still play a role, but attacks largely originate elsewhere. Identity is typically the first choke point in the attack chain and often the weakest link.

To understand how organizations deal with this reality, ID Dataweb partnered with CIO Dive's Studio to survey 150 U.S.–based security and IT leaders across Banking, Financial Services, Insurance, and Healthcare. All participants held manager-level roles or higher, with nearly half serving in C-level or VP/Head positions. The research drilled into how organizations perceive identity risk, how confident they are in their defenses, and what is stopping them from achieving stronger security outcomes.

The results reveal an inflection point: **Awareness is high. Investment is ramping up. Yet confidence remains elusive, and critical blind spots persist.**

Top Takeaways

High awareness, low confidence

82% recognize the phrase "identity is the new security perimeter"—but only **17% are extremely confident in detecting identity-based threats.**

Defender focus lags attacker reality

Phishing (90%) dominates concern, yet **fewer than half report strong understanding of impersonation (40%) or AI-driven attacks (23%).**

Integration is the real blocker

The top barrier to identity-first security is fragmented identity systems (43%), not budget or tools.

Authentication does not equal assurance

Despite widespread MFA and biometrics, **just 13% are extremely confident in preventing account takeover and fraud.**

High awareness, low confidence

The phrase “identity is the new security perimeter” is well known. More than four out of five respondents report being extremely or very familiar with it. There is a strong awareness that identity can be central to modern security strategy, not an adjunct to network or endpoint controls.

What the data shows

Awareness is high **(82%)**, but extreme confidence drops sharply across detection and response **(17%)** and identity fraud prevention **(13%)**.

What this signals

Identity is widely recognized as the perimeter, but confidence collapses once organizations are asked to prove detection, response, or fraud prevention in practice.

Despite widespread awareness, respondents are candid about the limits of their confidence. Fewer than one-third are extremely confident that their organizations understand the full attack chain behind identity-based breaches. Fewer than one in five are extremely confident in their ability to detect and respond to identity-based threats. Extreme confidence plummets even more when respondents evaluate credential-only authentication.

The Confidence Cliff

Confidence erodes quickly as identity questions become more concrete.

The gap between recognition and readiness cannot be overstated. Many organizations believe they understand the problem. Far fewer believe they have fully addressed it.

This hesitation reflects real-world uncertainty, not a lack of skills. Attacks are more adaptive and less dependent on obvious technical exploits. High-level confidence is harder to justify. Security leaders know that identity attacks do not follow static patterns. They know legacy controls were not designed to provide continuous visibility into identity behavior across systems and roles. That uncomfortable gap cannot be ignored.

Action:

Shift identity strategy discussions from awareness and intent to measurable confidence in detection, response, and identity fraud prevention capabilities.

Where identity attacks are actually happening

When asked which identity-based techniques present the greatest risk, respondents unsurprisingly cite phishing and MFA fatigue. Compromised credentials, password spraying, and credential harvesting also rank highly.

Perceived top risks

- Phishing **(90%)**
- MFA fatigue **(71%)**
- Login authentication **(53%)**

Undervalued risk areas

- Impersonation **(40% rate their understanding as excellent)**
- AI-assisted attacks **(23%)**
- Help desk interactions **(27% prioritized)**

Despite this awareness, emerging attack methods such as SIM swapping, AI-generated content, and deepfakes ranked significantly lower. This disparity suggests that while organizations recognize identity as an attack vector, many remain focused on tactics that dominated earlier phases of the threat landscape. Clearly, a wider level of prudence is required.

Many of today's most dangerous identity attacks rely on impersonation and process abuse, not technical exploitation. Help desk interactions, emergency access requests, and trusted internal workflows are increasingly targeted. These methods bypass traditional authentication safeguards. AI has supercharged these techniques by removing telltale signs of fraud, such as poor grammar or inconsistent tone. Using AI, attackers can sound polished and professional.

The result is a growing mismatch between how attackers operate and where defenders focus. Organizations may believe they are addressing identity risk, but critical identity surfaces remain underprotected.

Action:

Expand threat modeling beyond phishing and credentials to include impersonation, help desk abuse, and AI-assisted social engineering tactics.

The reality of today's identity security posture

Most organizations surveyed have made meaningful progress in identity and access management (IAM). Centralized IAM platforms, MFA, conditional access policies, and identity governance tools are widely deployed. Identity and access management is the most frequently cited element shaping the modern security perimeter.

The state of identity security maturity

Despite near-universal reliance on IAM **(95%)**, only **15%** of organizations report programs mature enough to deliver continuous detection and automated response.

Most remain anchored in transactional controls:

- **70%** rely on identity verification
- **67%** use identity threat detection

Full optimization remains rare. For most organizations, identity security is still fragmented across tools, roles, and teams, limiting the ability to assess identity risk holistically.

A single individual may appear as a workforce user in one system, a privileged user in another, and a customer or contractor in a third. When identity context is fragmented in this way, visibility into identity misuse becomes difficult, even when controls are widely deployed.

As a result, many organizations rely heavily on authentication success as a proxy for security, without clear insight into how identities are being used, abused, or combined across environments.

Action:
Evaluate whether existing IAM investments provide insight into identity misuse and risk accumulation, not just access approval.

False Reassurance: “No breach” ≠ No risk

Seven in 10 respondents say their organizations have not experienced an identity-related incident in the past 12 months. At face value, this sounds like a good thing.

A false sense of security

- **71%** report no identity-related incidents in the past 12 months.
- Only **28%** are extremely confident they understand the full identity attack chain.
- A mere **17%** express extreme confidence in detecting and responding to identity-based threats.

Leadership Implication

When organizations report no identity incidents yet are unsure how identity attacks unfold or how early they would detect them, the issue is no longer deployment—it is **unverified trust** in controls that lack behavioral visibility.

A closer look tells another story. Many identity-based attacks do not trigger immediate disruption. Intruders remain undetected until data is exfiltrated, systems are encrypted, or identity fraud becomes obvious. When incidents are investigated, attention frequently centers on the point of impact. But the identity-driven steps that enabled access in the first place remain unaddressed.

Limited visibility into identity behavior makes it hard to spot identity as the root cause of an incident. This results in underreported or misclassified identity risk. Organizations are lulled into a false sense of security. The absence of detected incidents should not be interpreted as the absence of intrusion.

Action:

Reassess identity risk assumptions by examining whether current tools can surface identity-driven activity earlier in the attack chain.

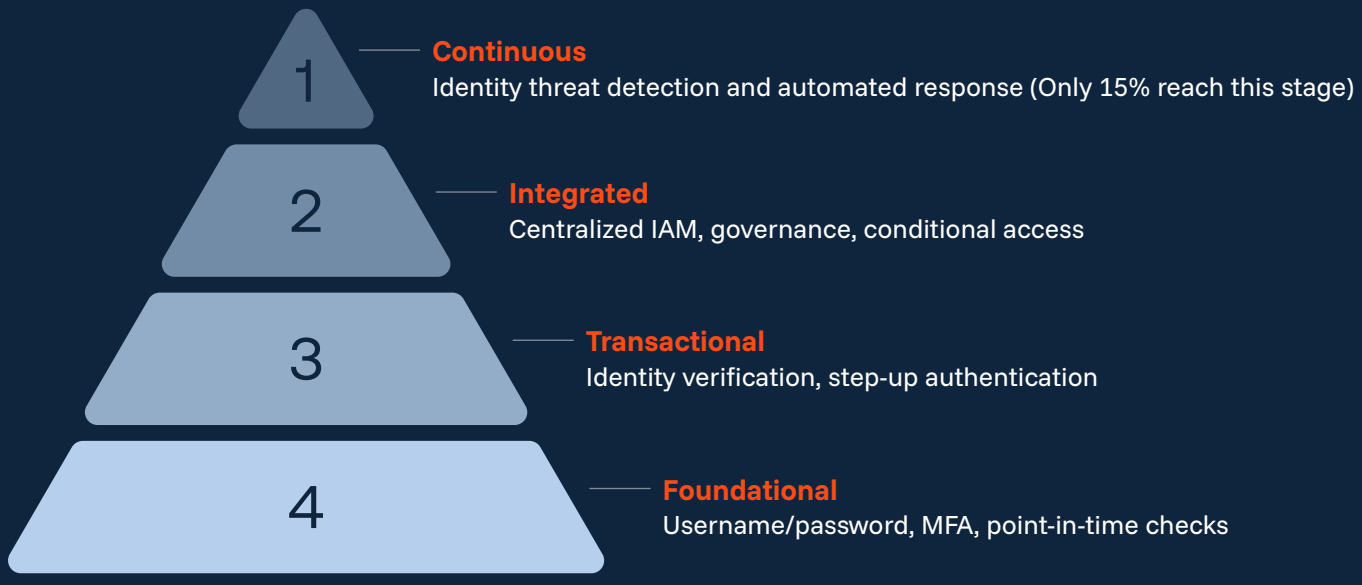
Verification vs. threat detection

Familiarity with identity verification and identity threat detection concepts is high among respondents. Many organizations use a range of verification methods, including passwords, biometrics, one-time passcodes, and authenticator apps. These controls are essential, but they are inherently transactional.

Familiarity does not equal maturity

- **83%** of respondents are extremely or very familiar with identity verification or identity threat detection concepts, but most still rely on foundational controls.
- Nearly all organizations use usernames and passwords **(93%)**, yet only **35%** have adopted continuous identity threat detection or risk scoring.

Identity security maturity snapshot



What does identity verification do well? It determines whether a user is who they claim to be at a specific moment. It evaluates signals associated with a single interaction. While this works for discrete events, it struggles to detect abuse that emerges across a spectrum of actions, identities, or systems.

Identity threat detection takes a broader view. Rather than evaluating isolated transactions, it continuously analyzes identity behavior, correlating signals across users, devices, locations, and time. This approach makes it possible to identify misuse patterns, even when individual actions appear benign.

The survey results suggest that many organizations conflate these concepts or overestimate the protection provided by point-in-time checks alone. When facing sophisticated threats, this gap matters substantially.

Action:

Clarify the role of point-in-time identity checks versus continuous identity monitoring within the broader security architecture.

Confidence in preventing account takeover and identity fraud

Only a fraction of respondents express extreme confidence in their current identity verification or threat detection processes. Most describe themselves as very confident or somewhat confident. This hedging reflects uncertainty rather than assurance.

Confidence declines at the point of proof

- Only **13%** are extremely confident that their identity controls prevent account takeover and identity fraud, while **60%** describe themselves as very confident.
- Extreme confidence falls to just **5%** when evaluating credential-only authentication against modern attacks.

They hesitate for a good reason: fragmented identity data muddy the waters. When signals are dispersed across tools and teams, security staff must pivot to manual investigation and judgment calls. This increases the chances of false positives and missed indicators. The result? Eroded trust in automated response discourages more proactive controls.

Organizations are sandwiched between risks: introducing excessive friction that degrades user experience and allowing suspicious activity to proceed unchecked.

Action:

Identify where fragmented identity data undermines confidence in fraud prevention and prioritize consolidating identity risk signals.

High-risk identity moments that matter most

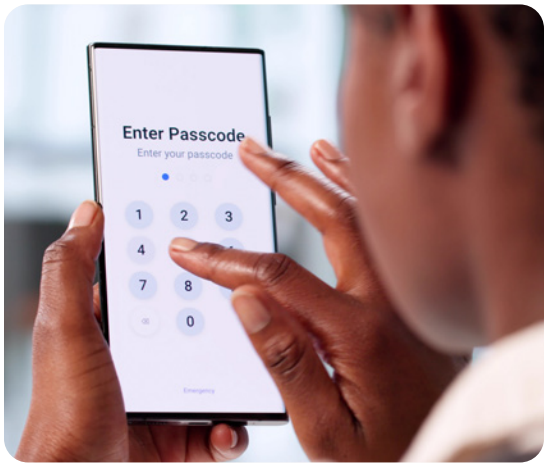
What are the top identity security concerns? Respondents identify login authentication and high-risk transactions, such as profile or payment changes, as their biggest worries. Password resets and help desk interactions also rank highly, though they receive less attention in practice.

Risk is concentrated, but not evenly defended

- Login authentication is the most cited identity risk scenario **(53%)**, followed by high-risk transactions such as profile or payment changes **(45%)**.
- Yet only **27%** prioritize help desk interactions, despite their growing exploitation by attackers.

This is where identity context matters most. A login attempt may be routine, but the same credentials used to change account details or request elevated access carry greater risk. Without continuous context, things get sloppy. Organizations rely on static rules or blanket controls that apply friction broadly rather than precisely.

Risk-based escalation depends on understanding how identity behavior changes across scenarios. The survey findings underscore the need for identity security approaches that adapt dynamically rather than treating all interactions equally.



Action:

Apply risk-based escalation to high-impact identity moments such as logins, profile changes, and help desk interactions.

What's holding identity-first security back

One obstacle rises above all others to establish identity as the core security perimeter: lack of integration. This challenge is both technical and organizational.

Fragmentation is the primary barrier

Obstacles to identity-first security:

- Lack of integration **43%**
- Budget constraints or legacy infrastructure **30%**
- Unclear ownership **9%**

Fragmentation is reinforced by organizational design. When identity risk signals generated by HR, IT, and IAM remain outside security workflows, identity risk accumulates silently, regardless of how many controls are deployed.

Budget constraints, skill shortages, and user resistance further complicate efforts to modernize identity security. However, these challenges are secondary to the visibility and coordination gaps created by fragmented systems and siloed ownership.

Action:
Address integration and organizational silos as security risks, not just operational inefficiencies.

Investment trends and the road ahead

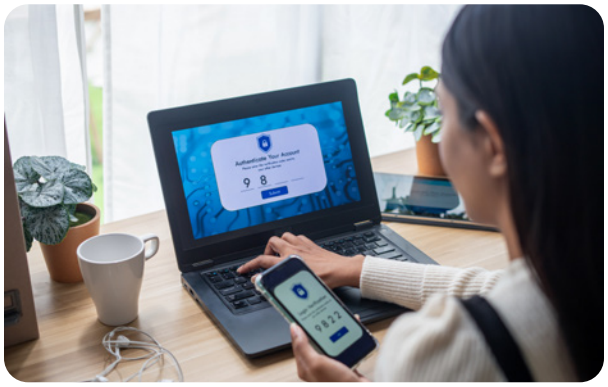
Identity security spending is expected to increase. Platform consolidation and identity governance improvements are getting the most attention. This reflects a desire to simplify environments and regain control over identity sprawl.

Investment is rising, with a focus on simplification

- **64%** expect identity security spending to increase in 2026.
- Rather than adding new tools, respondents prioritize identity platform consolidation **(39%)** and identity governance improvements **(35%)**.

Adoption of identity threat detection and risk mitigation is growing, but it's uneven. Many organizations approach identity maturity incrementally, layering new controls onto existing frameworks. Yet attacker tactics are evolving faster than this stepwise progression.

The findings suggest that organizations are beginning to question whether gradual evolution is enough. This makes sense since identity attacks are more adaptive and less predictable than ever. Time is not a luxury.



Action:

Align identity security investments around platforms and governance models that reduce complexity while increasing visibility.

Closing the confidence gap

The survey points to a clear conclusion: Awareness alone does not reduce risk. Confidence comes from visibility, integration, and the ability to detect misuse before damage occurs.

Identity maturity remains the exception

- Only **15%** report a mature identity posture with continuous detection in place.
- **29%** plan to deploy identity threat detection in the next 12–18 months.
- Extreme confidence remains below **30%** across all identity security capabilities measured.

Identity-first security delivers measurable value by addressing the earliest stages of the attack chain. By identifying anomalous identity behavior across systems and roles, organizations can intervene before attackers gain persistence or escalate privileges. This approach does not replace existing investments. It strengthens them by improving both security outcomes and user experience.

Closing the confidence gap requires moving beyond static authentication toward continuous identity threat assessment. It also requires breaking down organizational silos so identity risk signals can be evaluated in context.

Action:

Move from authentication-centric defenses to continuous identity threat detection to close the gap between attacker speed and defender response time.

Identity security at an inflection point

Identity has become the most actionable control point in cybersecurity. Organizations recognize this shift, but that alone has not delivered confidence. Fragmented tools, limited visibility, and evolving attacker tactics continue to undermine assurance.

The findings in this report show a market in transition. Security leaders are realistic about their limitations and increasingly willing to invest in identity-focused defenses. The next phase of identity security will be defined not by additional checkpoints, but by the ability to understand identity behavior holistically and respond with precision.

For organizations seeking meaningful risk reduction, the path forward lies in turning identity awareness into identity confidence.

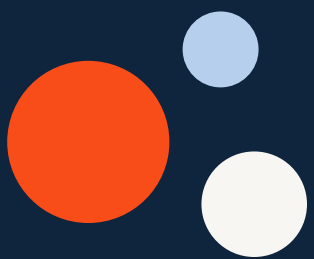
ID Dataweb

ID Dataweb™ helps enterprises stay ahead of identity fraud and account-related threats with real-time detection and mitigation while maintaining a seamless experience for their workforce, third parties, and customers.

The ID Dataweb SaaS platform combines adaptive identity verification methods, behavioral analytics, device and credential intelligence, and risk scoring. Backed by AI and expert insights, these capabilities proactively stop identity-based attacks, protect revenue, and strengthen compliance.

Unlike static legacy identity tools, ID Dataweb delivers dynamic, multi-layered risk orchestration that adapts to evolving threats. Its low-code, cloud-native services deploy quickly, integrate seamlessly with existing IAM systems, and align with each customer's policies.

Learn more



Expert led.
Impact driven.

Studio is Informa TechTarget's global content studio offering brands an ROI rich tool kit: Deep industry expertise, first-party audience insights, an editorial approach to brand storytelling, and targeted distribution capabilities. Our trusted in-house content marketers help brands power insights-fueled content programs that nurture prospects and customers from discovery through to purchase, connecting brand to demand.

Learn more