

The KYE & Workforce Identity Crisis Report

A Practical Report to Securing Workforce Identity in the Age of AI and Impersonation

New research from 1,002 U.S. and UK senior IT and security decision-makers reveals the growing gap between workforce identity risk and workforce identity assurance.



ENTRUST
SECURING A WORLD IN MOTION

EXECUTIVE SUMMARY

The Gap Between Knowing and Verifying

You Verify Customers. Why Not Employees? Ask a security leader whether insider risk matters and the answer is nearly unanimous. Ask whether they could catch an imposter walking through their own digital front door, and the confidence evaporates. That distance, between what leaders know and what they can truly stop, is the story this research aims to tell. It surfaced three findings every security leader should know:

1. Workforce identity is now a board-level security problem.

96% of leaders call insider risk significant to their organization, and not a single respondent dismissed it outright. Few cybersecurity concerns achieve that kind of unanimity. Insider risk has become a business risk with boardroom visibility.

2. Organizations see the risk but can't confidently verify people.

Awareness hasn't translated into assurance. Not one moment in the employee lifecycle earned more than 46% "very confident" marks for identity verification, and confidence sinks to 31% for contractor and temporary access – the very users organizations know the least. Nearly everyone agrees stronger employee verification is needed, but how to achieve it remains unclear.

3. Attackers have stopped picking locks and are now borrowing faces.

Social engineering now tops the workforce identity threat list, AI-enabled impersonation is accelerating, and the softest targets aren't servers or endpoints anymore. They're people: new hires, contractors, remote workers, and help desks.

Workforce identity has become the missing layer of enterprise security.

Workforce identity has become the missing layer of enterprise security.

INTRODUCTION

Why Know Your Employee Matters Now

Passwords confirm what someone knows. Devices confirm what they have. But neither confirms who someone actually is. That unverified layer, the real human behind the login, is where attackers now see an opportunity.

For two decades, organizations have poured investment into passwords, multi-factor authentication (MFA), privileged access management (PAM), identity and access management (IAM), and endpoint security. Every one of those technologies does their job. But every one of them only answers two questions: What does someone know, and what does someone have?

They do not answer another important question: Who is the human behind the login?

That blind spot is today's attack surface.

The entire authentication stack was built to validate identification cards, credentials, tokens, and devices, on the assumption that the right identification implies the right person. Attackers noticed the assumption and took aim.

Enter Know Your Employee

Know Your Employee (KYE) is the practice of continuously verifying that every member of the workforce is who they claim to be, at the point of hire, throughout the employee lifecycle, and at every consequential moment where trust, access, or identity must be established.

Banks have spent decades verifying customers because they know trust is never assumed. Know Your Employee applies the same principle to the workforce, bringing identity assurance to the people organizations trust most.

Workforce Identity Risk Follows the Employee Lifecycle

Identity risk doesn't begin at login, and it doesn't end once access is granted. It follows the employee lifecycle from hiring and onboarding to account recovery, remote access, role changes, and offboarding. Each of these moments requires an organization to answer the same question: Is this person really who they claim to be?

Increasingly, attackers are betting the answer is no.

The Verification Gap Across the Employee Lifecycle

Most identity controls verify a credential, device, or authentication factor. They don't verify the human behind them. That's why onboarding, account recovery, help desk interactions, and contractor access have become attractive targets for attackers. Rather than breaking through security controls, they're increasingly finding ways around them by impersonating trusted users.

To understand how organizations are responding to this challenge, Entrust commissioned independent research among 1,002 senior IT and security decision-makers across the United States and United Kingdom. The findings indicate a persistent gap between awareness of workforce identity risk and confidence in the ability to control it.



Table of Contents

The Threat Landscape: Attackers Have Found the Weakest Link: Humans	5
The Confidence Gap: Every Step Reveals Another Gap	6
The Password Paradox: Guarding the Door With the Lock They Fear Most	7
Where the Gaps Live: Walking the Lifecycle: Five Blind Spots	9
The Reality: Not a Forecast, But a Field Report	10
The Accelerant: AI Made Impersonation a Product	11
The Shift: KYE Is Moving Into the Security Mainstream	12
Putting It Into Practice: Building a Practical KYE Framework	13
Conclusion: The Future of Identity Security Is Workforce Identity	14

THE THREAT LANDSCAPE

Attackers Have Found the Weakest Link: Humans

Organizations know the login but not the person.

The biggest challenge in modern security is a consequence of success. Networks are hardened. Devices are managed. Applications are patched. Credentials are vaulted. Combined, they make those physical access routes harder. So attackers did what attackers always do: They moved to the surface nobody had hardened.

Today, attackers arrive posing as new hires clearing background checks, contractors requesting system access, and employees locked out of accounts. Instead of breaching the firewall, they call the help desk. Instead of cracking the password, they reset it, moving through account recovery workflows built to be helpful and staffed by people trained to be accommodating.

The tactics vary, but the objective is the same – to gain trusted access. Some attackers play the long game, securing employment under a stolen or synthetic identity and spending months collecting paychecks while quietly exfiltrating source code, customer data, and intellectual property, or establishing persistence for future attacks. Others move fast, using social engineering to bypass help-desk controls, reset credentials, and gain immediate access

to interconnected systems through single-sign-on (SSO). In both cases, the damage begins only after the attacker is recognized as a legitimate employee.

The research shows this shift is already happening:

- Phishing and social engineering targeting employees is the No. 1 concern, cited by 46% of security leaders
- Credential compromise follows at 43%, with privileged access misuse (34%), account takeover and impersonation (33%), negligent employee behavior (32%), and malicious insider misuse (32%) clustered tightly behind
- 34% have already investigated employee impersonation incidents, showing this isn't a looming threat but is actively happening

The ranking matters less than the pattern. Workforce identity risk is a collection of threats exploiting the same blind spot. Assuming that an employee account always belongs to the employee makes it harder to defend.

46%

Cite phishing and social engineering as the No. 1 concern

43%

Credential compromise is the second-most cited concern

34%

Have investigated employee impersonation incidents

The Confidence Gap

Every Step Reveals Another Gap

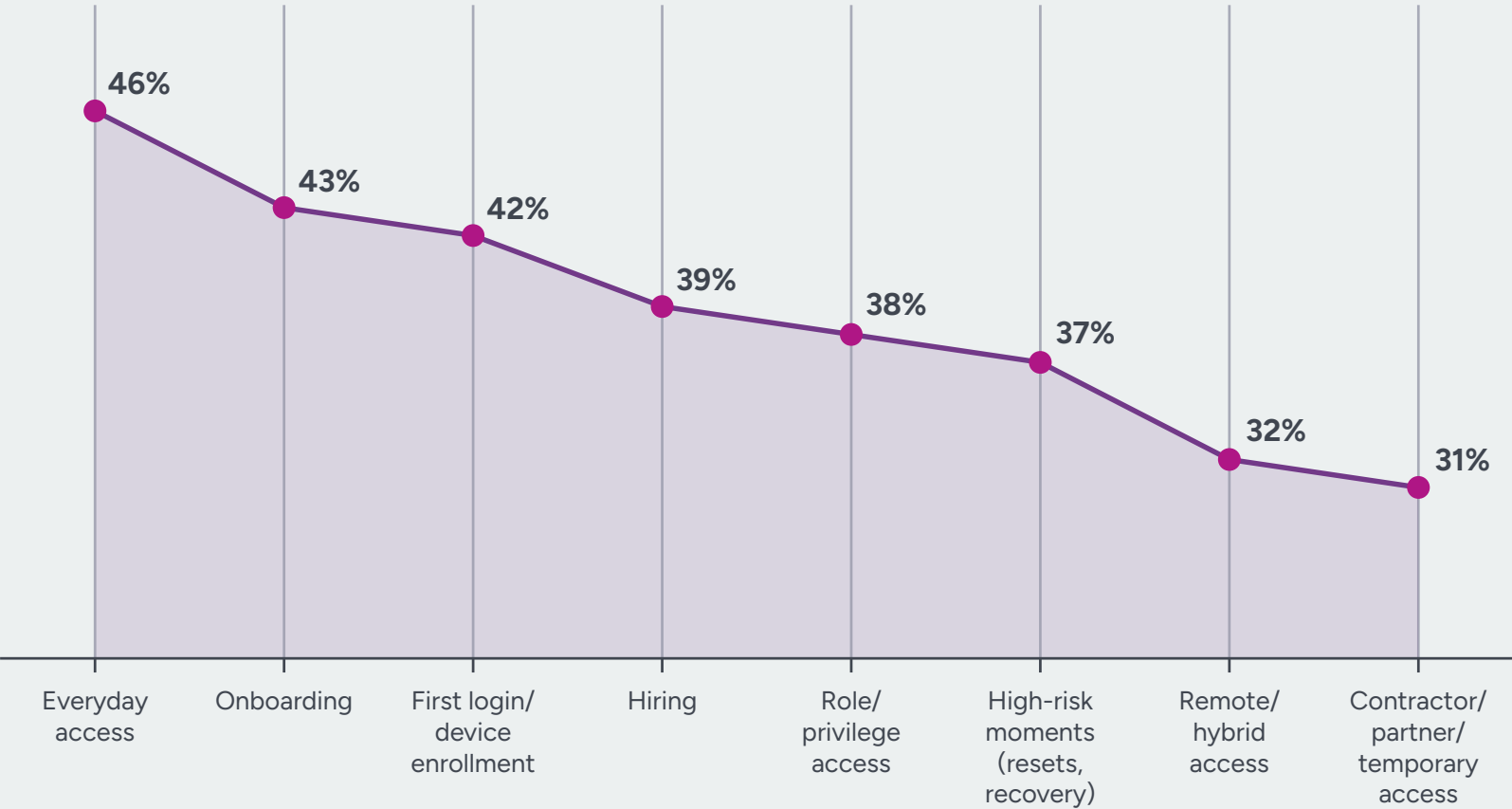
Security leaders were asked a simple question: How confident are you that your organization can reliably verify who is accessing systems at each moment of the employee lifecycle? Viewed together, their answers form a staircase, and every step leads downward.

Start at the top of the chart: Even the highest-scoring moment, everyday access, earns just 46% confidence. The strongest point in the lifecycle is barely a coin flip. Now look at the bottom. Confidence erodes exactly where identity is most fluid and hardest to verify: Account recovery, remote/hybrid access, and third-party contractor access. These are the moments organizations trust least and attackers target most.

Fewer than half of leaders believe they can reliably verify who is accessing their systems day to day, and fewer than 2 in 5 feel confident at hiring, privilege changes, and high-risk moments like account recovery.

The result is a lifecycle-wide trust problem. Confidence never exceeds 46%, and it falls steadily at the moments where attackers face the fewest obstacles and organizations have the least certainty about who is behind the account.

Confidence in Identity Verification
Falls at High-Risk Workforce Moments



Only 31% of security leaders are very confident verifying contractor, partner, and temporary worker access.

The Password Paradox

Guarding the Door With the Lock They Fear Most

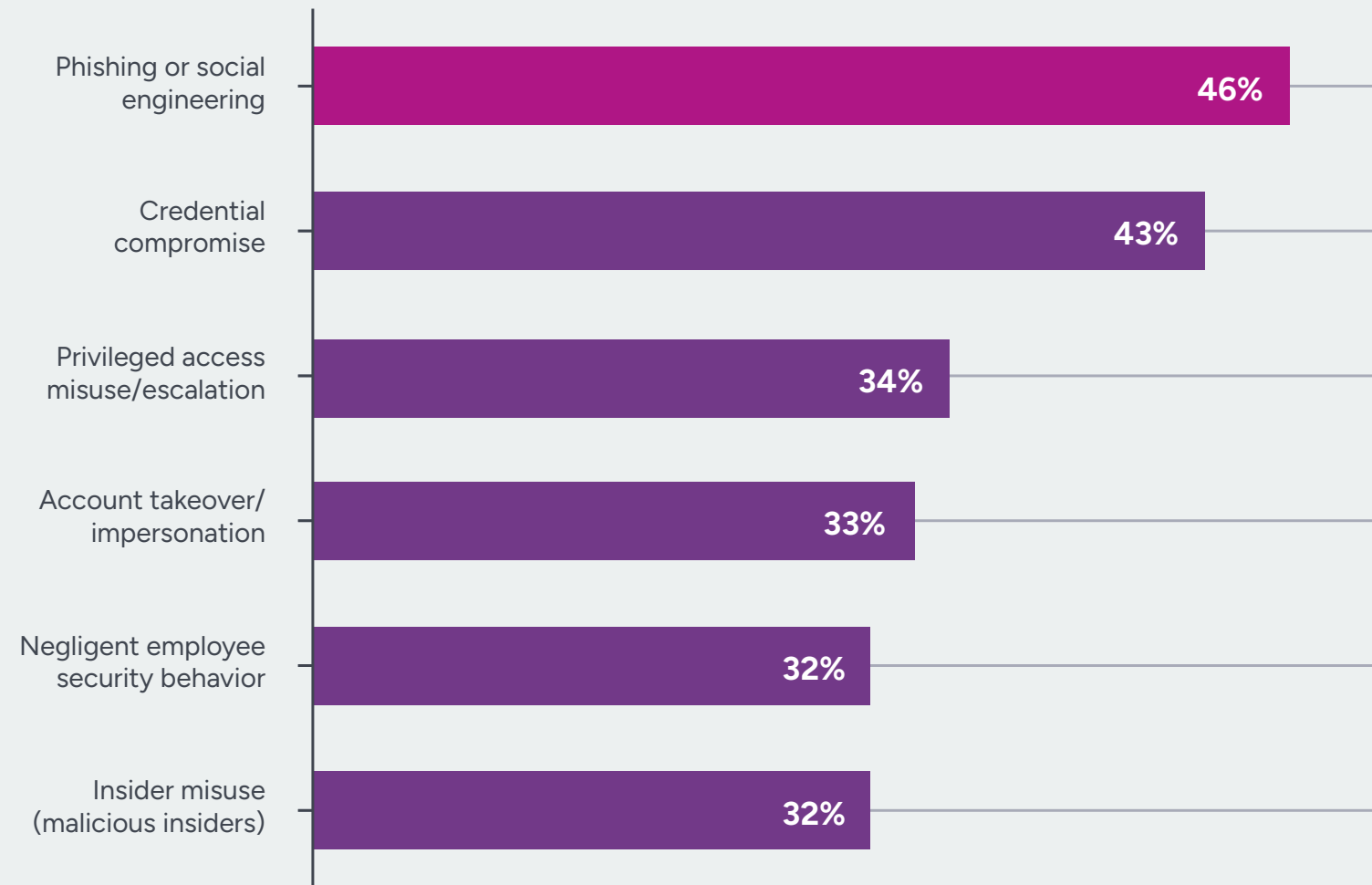
If you asked security leaders to name the identity threat they worry about most, social engineering would top the list. Nearly half (46%) cite phishing and other social engineering tactics as a leading concern, just ahead of credential compromise at 43%.

The two are closely connected. Social engineering is rarely the end goal. It's the means of exploiting trust. A convincing phishing email, a well-timed call to the help desk, or a carefully crafted pretext can persuade someone to reset a password, bypass a control, or grant access they otherwise wouldn't. The credential compromise security leaders fear is often the result of the social engineering they fear even more.

Now consider how those same organizations authenticate employees. The most common answer is usernames and passwords, at 45%.

Consider that disconnect. The threat organizations fear and the control they rely on are often closely linked. Organizations continue to rely heavily on the very credential-based controls attackers most frequently target.

Identity-Related Threats That Concern Security Leaders Most

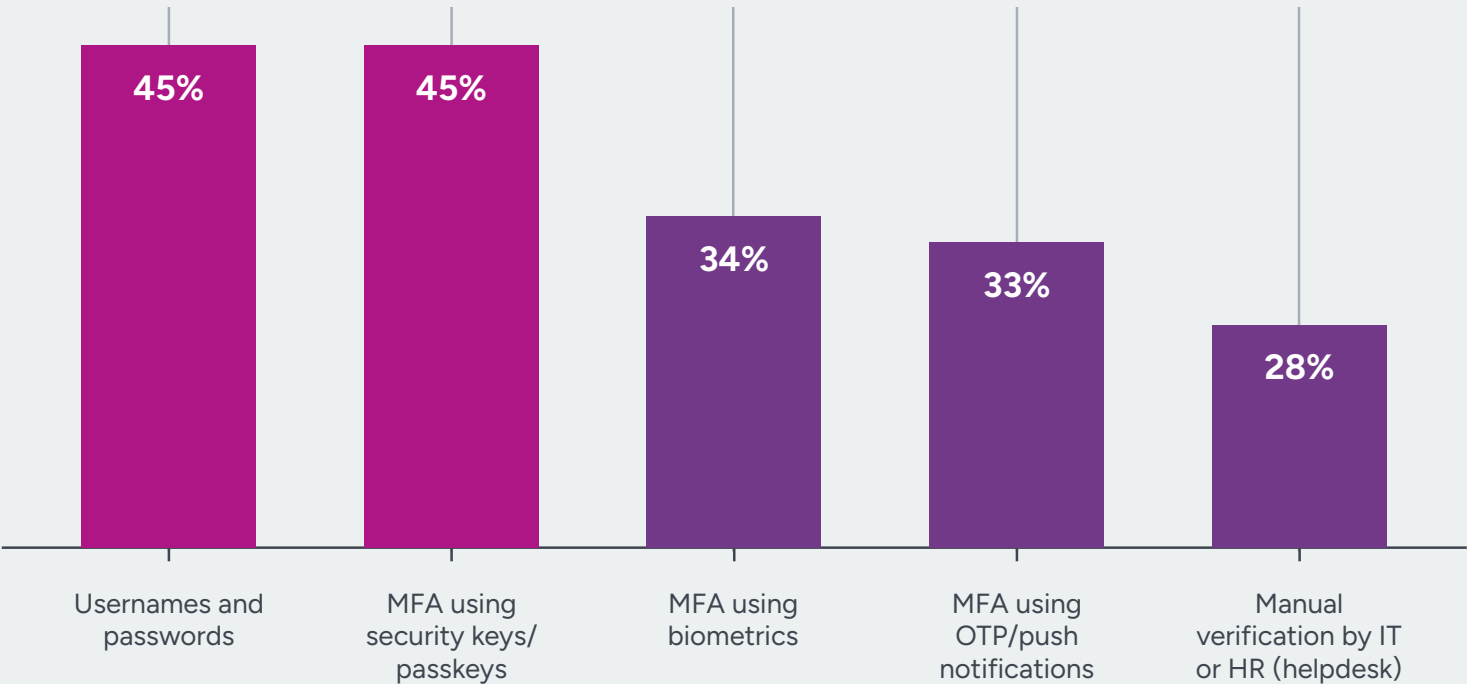


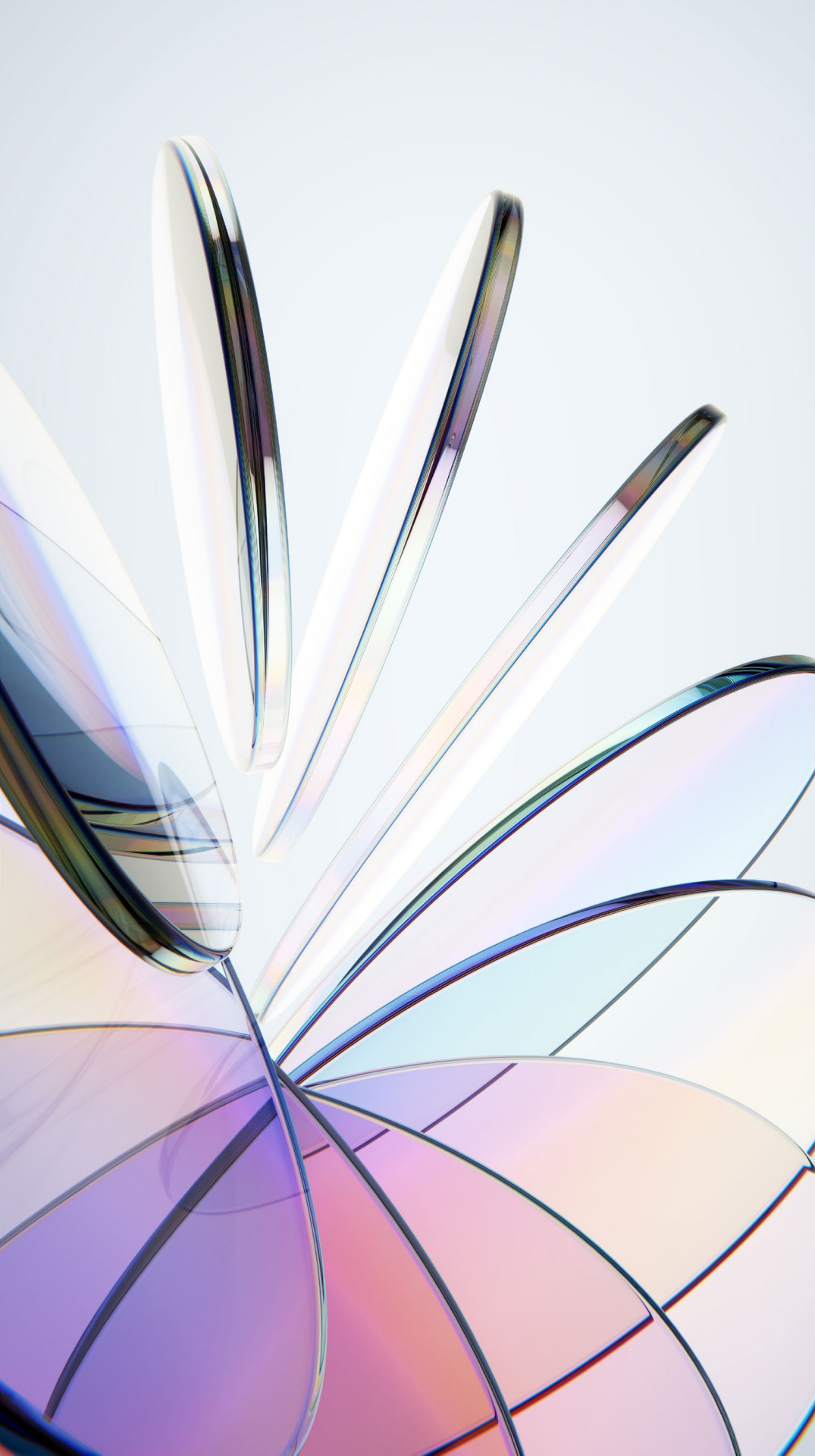
The Full Authentication Picture

There's no single dominant approach, and even the stronger methods share a limitation: They confirm a credential or a device, not a person. Passwords verify what someone knows. MFA verifies what someone has. Even stronger authentication methods validate a credential, device, or biometric factor. What they don't necessarily verify is the human behind them. Meanwhile, more than a quarter of organizations still fall back on manual IT or HR verification, a judgment call, made under pressure against increasingly convincing impersonators.

This is the password paradox in its simplest form:
Organizations recognize this risk yet still rely on controls
that verify credentials more reliably than they verify people.

Primary Methods Organizations Rely on to Authenticate Employees





Where the Gaps Live

Walking the Lifecycle: Five Blind Spots

Follow an employee's journey from application to account recovery, and the blind spots reveal themselves in sequence. The risk appears before an account even exists, during the hiring process itself.

Hiring: The Fear Arrives Before the Badge Does

30% of leaders worry about fraudulent hires, yet only 39% feel confident verifying identity at hiring. The risk starts before day one. Candidate fraud has already affected 28% of organizations but remains one of the least-discussed threats.

Onboarding: The First Access Gap

29% have already investigated access abuse tied to onboarding or role changes, yet onboarding confidence sits at just 43%. The onboarding gap is already producing incidents.

Account Recovery: The Attacker's Favorite Route

Social engineering is the top workforce identity threat (46%), and it targets the workflow organizations trust least: Account recovery, where confidence sits at just 37%. Attackers don't need to bypass security controls if they can convince someone to let them in.

Contractor and Third-Party Access: Trust Without Acquaintance

At 31%, contractor, partner, and temporary access earns the lowest confidence score in the entire study. At the same time, 96% of leaders view insider risk as significant. Organizations recognize the risk, yet confidence is lowest for the people they know least and increasingly depend on.

AI Impersonation: The Visibility Gap

54% are actively watching AI-enabled impersonation threats, but only 39% measure and report on them. Awareness has arrived faster than accountability, leaving many organizations unable to quantify a risk they already know is growing.

When viewed together, these blind spots are too consistent to be a coincidence. Confidence falls where identity is hardest to pin down and exactly where attackers aim.



The Reality

Not a Forecast, But a Field Report

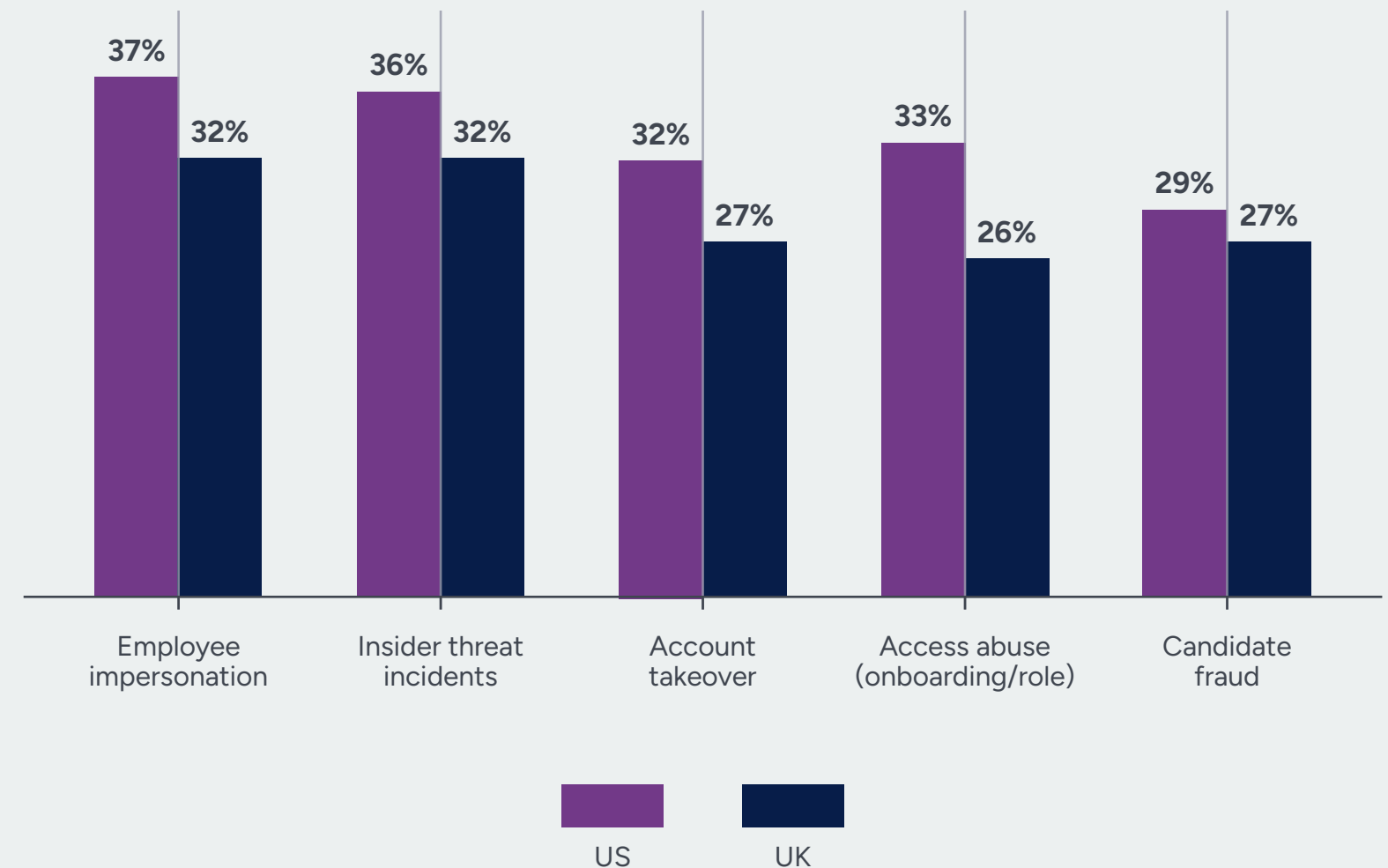
Set aside the forecasts and worst-case scenarios, and one number remains: 91% of organizations experienced an identity-related incident or near miss in the past two years. **Just 1 in 11 escaped clean.** For 9 out of 10 security leaders, workforce identity attacks are a recent memory.

Two findings deserve a closer look. First, candidate fraud has already affected 28% of organizations, yet ranks among the lowest-cited concerns. It's happening more than it's feared – the very definition of a blind spot.

Second, exposure changes depending on where and how people work: U.S. organizations report higher incident rates than the UK across every category, and fully remote organizations record the highest levels of impersonation, insider threats, and candidate fraud, at 37% each. The more remote an organization becomes, the wider its identity gap tends to grow.

For a security leader, the takeaway is blunt: This moves the risk from “possible” to “probable.” When a third of your peers have already investigated employee impersonation, and more than 9 out of 10 have experienced an identity-related incident or near miss, doing nothing gets harder to justify to a board.

Incidents Experienced in the Past Two Years



The Accelerant

AI Made Impersonation a Product

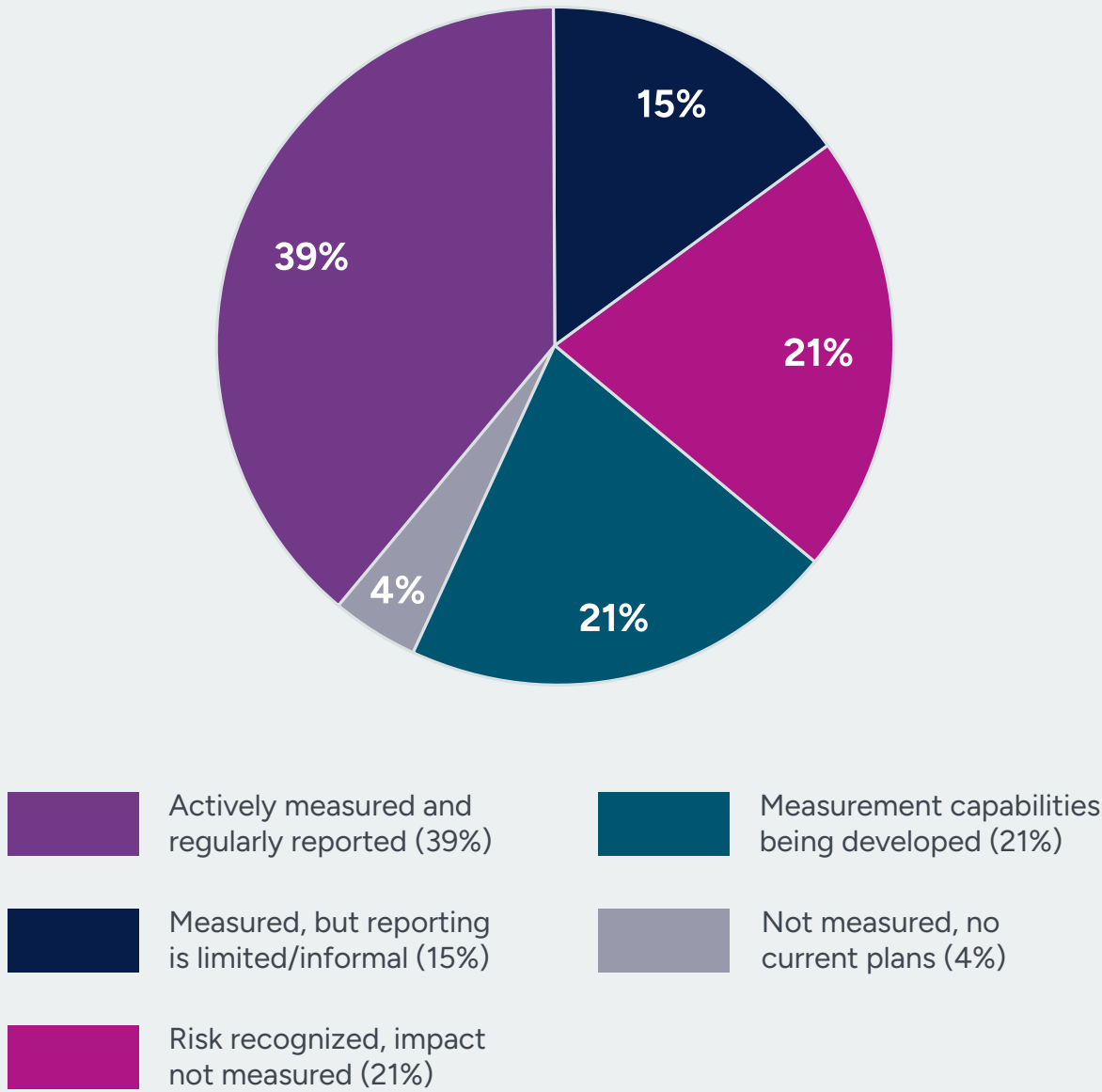
Impersonation used to require craft. Now it requires a subscription. Generative AI has industrialized the forgery of people: Deepfaked faces in video interviews, cloned voices calling the help desk, forged documents that pass casual review, synthetic candidates, and executives who never sent that urgent request. Every technique aims at the same target: The manual verification and human judgment that legacy processes still depend on.

Security leaders know the threat is coming, but what many still lack is a consistent way to measure its impact.

Over half (54%) are monitoring AI-enabled impersonation in some way, and only 4% have ruled out measuring it altogether. Yet just 39% actively measure and report on its impact. The rest sit in the middle: Aware of the risk but not yet managing it.

Boards are already starting to ask about deepfake and synthetic identity risk. That makes this a reporting gap leaders will soon be expected to close. As AI-enabled impersonation grows, measuring identity risk will become the first step toward managing it.

How Organizations Measure AI-Enabled Impersonation



The Shift

KYE Is Moving Into the Security Mainstream

Not long ago, Know Your Employee (KYE) was a niche concept borrowed from banking compliance. The market has since made up its mind: 59% of security leaders now call KYE a key part of modern identity security strategy. Another 23% see it as essential for high-risk roles and workflows, and 13% call it important but not yet prioritized. Only 3% dismiss it outright. More than 8 in 10 see value in KYE as either a key modern identity strategy or essential for high-risk roles and workflows, meaning the debate over whether to verify the workforce is effectively over. The real question is how to close the gap leaders already feel.

59% call KYE core strategy, yet 45% still authenticate employees with passwords.

So what's really in the way?

Not conviction. Not even the price tag. The top barriers cited are tool sprawl (17%), the complexity of existing tools (17%), and fragmented, on-premises, or homegrown identity systems (13%). Limited budget trails at 11%, and lack of board buy-in barely registers at 5%. Only 10% report no barrier at all.

If you read those numbers together, the diagnosis writes itself: The blocker isn't belief or budget, but fragmentation. Identity data and workflows are scattered across HR systems, IAM platforms, PAM tools, and directories, and leaders are understandably reluctant to bolt on yet another disconnected system.

And who owns the problem?

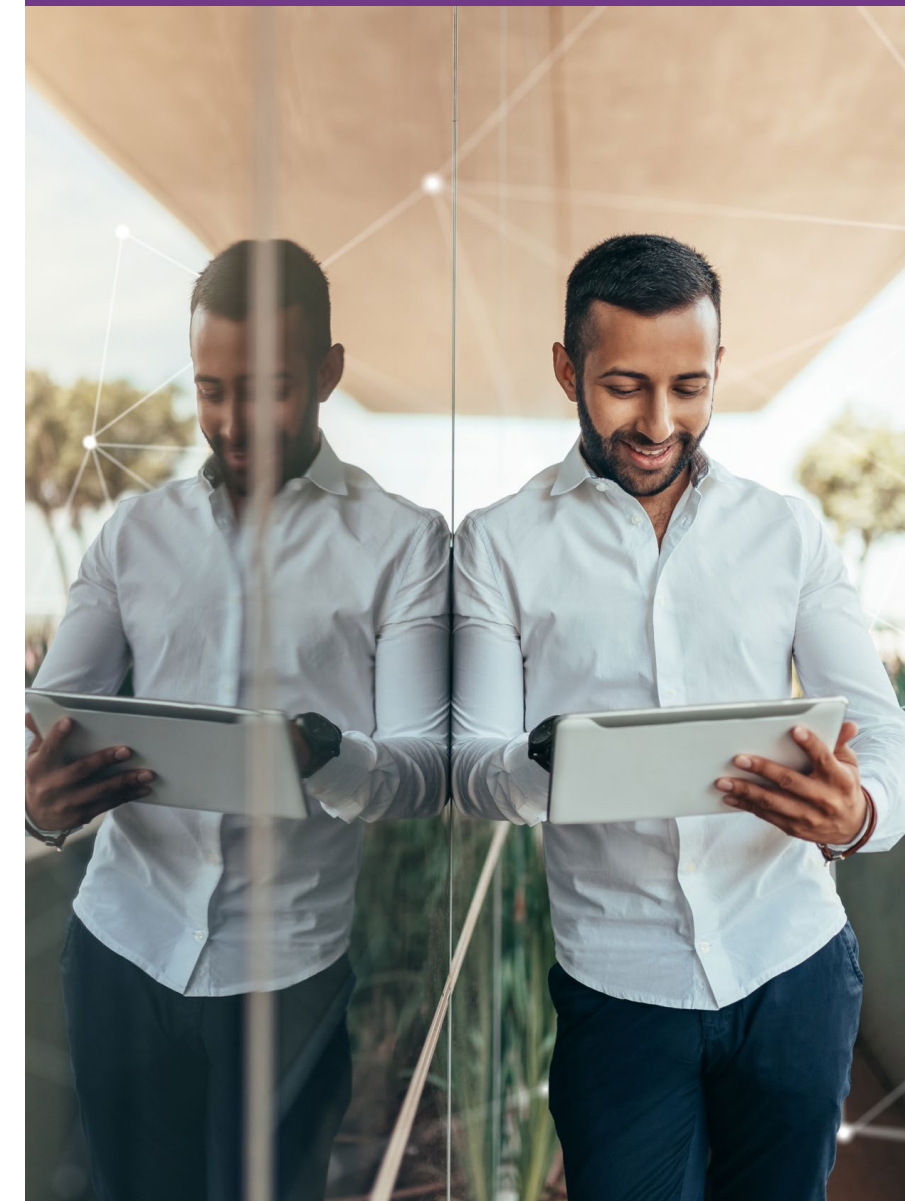
45% say the CISO or security team holds primary responsibility for workforce identity. But 22% point to IT, 20% to the CIO, and just 8% say the CHRO or HR team owns it, even though HR runs hiring and onboarding, where the gap begins. Only 4% describe ownership as genuinely shared. Everyone assumes someone owns workforce identity, but few agree on who.

Even support for KYE varies across the organizations expected to champion it. CISOs are the strongest advocates, with 65% calling KYE a core identity strategy, while IAM leaders, the teams often tasked with implementation, are the least convinced at 48%. The people driving the strategy and the people expected to implement it are not always fully aligned.

That seam between hiring and identity ownership is just the point where accountability and risk can fall through the cracks.

Security leaders already understand the value of workforce identity verification, but they need a way to put it into practice within fragmented environments, complex toolsets, and unclear ownership structures. The answer is through better integration.

59% call KYE core strategy, yet 45% still authenticate employees with passwords.





Putting It Into Practice

Building a Practical KYE Framework

Everything this research surfaces – the confidence gap, the password paradox, the measurement gap, the ownership muddle – points to the same underlying problem: Organizations recognize the risk, but their tools, processes, and structures weren't built to verify the real person. Closing that gap requires four disciplined moves.

- 1 Secure the high-risk moments first:** Confidence doesn't fail evenly. It collapses at specific moments: Contractor access (31%), remote and hybrid access (32%), and account recovery (37%). Start where confidence is lowest and attackers are most active.
- 2 Start at day one, not after the fact:** The risk begins at hiring. Verifying identity during hiring and onboarding establishes a trusted baseline before someone ever logs in, closing the earliest and most overlooked gap in the workforce lifecycle.
- 3 Verify the person, not just the credential:** Passwords and MFA, the two most-used methods at 45% each, verify a credential, device, or factor, but they don't necessarily establish that the person presenting it is the legitimate employee. Adding identity verification addresses the weakness passwords and MFA leave behind, providing a direct countermeasure to AI-driven impersonation and deepfakes.
- 4 Integrate – don't add another silo:** Identity verification works best when it integrates with existing IAM, HR, and ITSM systems. That approach reduces complexity, minimizes tool sprawl, and makes KYE a natural extension of existing identity workflows.

The market accepts that workforce identity needs stronger verification, but what remains is the real work: Embedding it into the systems, workflows, and decisions where identity must be trusted.

Conclusion

The Future of Identity Security Is Workforce Identity

Across 1,002 senior security leaders, the research keeps arriving at the same conclusion. Organizations recognize the risk almost universally. Insider threats worry 96% of respondents. Impersonation is growing. AI is accelerating everything. Yet confidence collapses in the moments attackers deliberately target because the tools organizations rely on were built to verify credentials, not people.

For years, that unverified layer was survivable, but AI-enabled impersonation ends the grace period. When a face, a voice, and a resume can be synthesized on demand, the only durable control is the ability to verify the human behind critical workforce interactions, at the moments when trust is being tested.

Organizations expect stronger verification to reduce security incidents (51%), fraud (46%), and operational inefficiencies (45%). Ultimately, the value of workforce identity verification is confidence: Confidence that the person requesting access, recovering an account, or performing a sensitive action is who they claim to be.



✓ Bring Identity Assurance Into the Moments That Matter

Entrust Workforce Identity Verification helps organizations establish confidence in the real person behind a workforce interaction.

✓ Establish a Trusted Identity

Verify employee identity during hiring and onboarding to create a reliable foundation before access is granted.

✓ Verify Identity Beyond Onboarding

Extend identity assurance into high-risk workforce interactions such as help-desk requests, account recovery, remote access, and other moments where trust matters most.

✓ Help Defend Against Sophisticated Impersonation

Verify the actual person, so an AI-generated face or voice can't get through when legacy checks fall short.

✓ Connect Verification to Existing Workflows

Integrate identity assurance into existing workflows and authentication journeys without treating identity verification as a separate, disconnected exercise.

The technology to verify people already exists.
The challenge now is putting it where identity actually gets tested.

Assess Your Workforce Identity Gaps

See how modern [workforce identity verification](#) and [KYE](#) solutions from Entrust can help establish trust across the employee lifecycle, from hiring through account recovery.



ABOUT ENTRUST

Entrust fights fraud and cyber threats with identity-centric security that protects people, devices, and data. Our comprehensive solutions help organizations secure every step of the identity lifecycle, from verifying identity at onboarding to securing connections and fighting fraud in everyday transactions. Ongoing monitoring supports compliance and safeguards keys, secrets, and certificates. With a foundation of identity-centric security, our customers can transact and grow with confidence. Entrust has a global partner network and supports customers in over 150 countries.

For more information, visit entrust.com.