Omdia
by informa techtarget

Controlling Identity Risk:

Detecting and Mitigating Identity Threats

Author: Todd Thiemann

February 2026

Contents

Introduction

Identity lies at the root of most enterprise data breaches and digital fraud incidents. Adversaries rarely hack their way in. Instead, they log in using weak, stolen, or otherwise compromised credentials, often obtained through social engineering, to achieve malicious goals.

Most identity verification approaches today focus narrowly on authentication. They attempt to confirm that a user is who they claim to be using relatively weak mechanisms such as passwords or traditional two-factor authentication (2FA). This model places nearly all trust in the credential itself. While existing solutions may address individual use cases, they struggle to scale across multiple identity scenarios and often fail to integrate seamlessly with existing processes and IT infrastructure.

As a result, enterprises seeking to reduce identity fraud costs and mitigate cyber risk across customer, partner, and workforce identities must reevaluate their identity verification strategies. A more holistic approach is required. This approach should emphasize continuous identity threat detection and risk-based mitigation to effectively combat identity-driven threats targeting both internal workforce identities and external customer and partner identities.

Moving Beyond Static Identity Verification

As attackers adopt increasingly sophisticated techniques, from multifactor authentication (MFA) bypass to SIM swapping to "socially engineering" help desk staff, organizations face growing exposure in areas that are often overlooked. Incidents such as the Scattered Spider attacks demonstrate that adversaries now deliberately target the weakest links in identity workflows, including customer service operations and employee onboarding processes. Traditional identity and access management (IAM) approaches, particularly knowledge-based authentication, are no longer sufficient against threat actors equipped with stolen data and advanced social engineering tactics.

In this environment, digital identity verification has become a critical capability for enterprises, both internally and externally. For workforce users and partners, organizations must verify high-risk identity workflows such as credential recovery and account changes. For external customers, enterprises must confirm that users are who they claim to be across a wide range of digital interactions. Whenever something of value is accessed, moved, or shared, identity verification is essential. This applies across consumer (B2C), business (B2B), and hybrid (B2B2C) use cases.

For example, financial institutions that have moved operations online must guard against third-party and synthetic identity fraud, which can increase costs in digital channels. As transactions have shifted online with the growth of digital commerce and services, verifying identities to prevent identity fraud and account-related threats has become critical. Any organization facilitating the movement of valuable assets online needs to verify transaction participants. This requirement spans multiple industries, including online banking, e-commerce, hospitality, travel, event ticketing, and eHealth.

Organizations validating identities, whether for internal workforce accounts or external customer accounts, go through an evolution as they mature and improve their operations (see Table 1).

Table 1: Identity Verification Maturity Model

Maturity stage	Maturity description
Credential-only authentication (Legacy approach)	Assumes that usernames and passwords are uncompromised and grants access to applications and networks based solely on their use.
Step-up authentication	Augments credential-based authentication with 2FA or MFA for high-risk interactions to increase identity assurance.
Identity verification (IDV)	Recognizes that credential-only authentication—and even some step-up methods—are no longer sufficient. Shifts focus from the credential to the person behind it, verifying that the legitimate user is the one leveraging the assigned credentials. IDV confirms a person's claimed identity using methods such as comparing a photo ID to a selfie with liveness checks, validating government records, or asking personal knowledge questions. While IDV typically evaluates individual interactions using authoritative identity sources and risk signals, it does not provide a holistic, continuous view across all digital interactions. Instead, it delivers solely a point-in-time check.
Identity threat detection and risk mitigation	The organization typically reaches this stage after experiencing that IDV alone can be bypassed. A multi-layered, holistic approach becomes necessary to detect identity fraud and account-related threats. This goes beyond IDV by analyzing the full pattern of transactions associated with a credential—as well as activity across other credentials in the environment. It includes a feedback loop, enabling continuous learning and fine-tuning of the decision engine. Identity threat detection and risk mitigation integrates adaptive identity verification, behavioral analytics, device and credential intelligence, and risk scoring. Together, these capabilities address both sides of the identity security challenge.

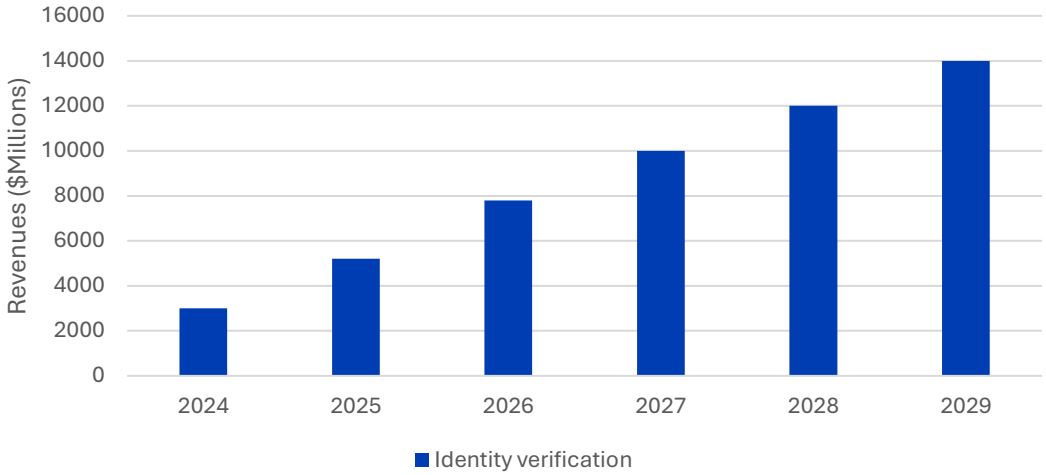
Source: Omdia

As technologies have improved to counter growing identity threats in a scalable and standardized way, verification methods have evolved from simple passwords to 2FA, secure certificates, and federated systems using identity standards like SAML, OAuth, and OpenID Connect to manage access.

The global market for identity verification solutions is expected to grow to $14 billion by 2029 according to Omdia analysis (see Figure 1).[1]

[1] Source: Omdia Research Report, *Fundamentals of Identity Verification*, June 2025.

Figure 1: World Market for Identity Verification (IDV), 2024-29



Source: Omdia

Threats have continued to increase in sophistication and resulting damage. The FBI reported that cybercrime, including identity fraud reached more than $16 billion in 2024, the highest number ever reported by the FBI's Internet Crime Complaint Center.

While enterprises have improved their defenses against workforce identity compromise, adversaries continue to socially engineer their way into obtaining valid credentials. Examples of successful attacks using this method include the MGM Resorts (2023), Hawaiian Airlines (2025), Allianz Life (2025) and Marks & Spencer (2025).

The spike in job candidate fraud involving North Korean tech workers has heightened awareness that identity fraud can start before someone becomes an employee. Mandiant reported on North Koreans acting as fake IT job candidates in 2024, and the US Department of Justice subsequently indicted 14 North Korean nationals in a scheme that generated $88M in illicit revenue from US companies.

These examples illustrate that, while organizations have begun adopting more sophisticated identity verification methods, significant gaps remain. Early identity verification adoption focused primarily on protecting against customer identity fraud, and only recently has this focus expanded to workforce and partner identities. Organizations should accelerate their maturity journey (see Table 1) and transition away from credential-only authentication to more robust and comprehensive authentication solutions. Doing so enables them to augment their existing IAM infrastructure with modern identity verification capabilities and to realize the optimal return on their security investments.

Understanding Identity Verification Approaches: Transaction-based vs. Holistic Identity Verification

"Identity verification" is typically an umbrella term that encompasses two distinct approaches. The first is transaction-based identity verification, which evaluates individual digital interactions to confirm an individual's identity. This method provides only a point-in-time assessment and does not account for insights gained from other digital interactions.

The second is a more holistic approach known as identity threat detection and risk mitigation. It incorporates traditional identity verification methods while also analyzing a broader set of digital transactions associated with a credential, and in some cases across multiple credentials. This approach enables the detection of anomalies and indicators of compromise, rather than relying solely on decisions based on a single transaction.

Customer Identity Verification

Identity verification enables enterprises to acquire more legitimate customers while effectively screening out fraudulent actors. Organizations rely on identity verification for a range of business objectives, including identity fraud prevention, secure digital onboarding, account takeover prevention, and strengthening customer trust.

Certain industries, such as financial services, are subject to regulatory requirements, including "know your customer" (KYC) and anti-money laundering (AML) obligations. These regulations require institutions to verify the identities of their customers to help deter identity fraud and illicit activity.

Identity Verification Business Drivers

- **Security and fraud prevention.** Organizations need to combat identity fraud, account-related threats, and impersonation scams and use identity verification to mitigate identity fraud risk and strengthen overall security.
- **Regulatory compliance.** Industries such as financial services, healthcare, and government face strict requirements related to KYC, AML, and data privacy regulations.
- **User experience.** Low-friction or frictionless verification experiences enable employees to be more productive and enable easier customer transactions.
- **Brand and revenue protection.** Identity fraud incidents and breaches result not only in financial losses but also in lasting reputational damage. Identity verification helps protect business continuity and preserve customer trust.
- **Long-term trust building.** Transparent and secure handling of identities fosters confidence in digital interactions and supports enduring relationships with users.
- **Global digital transformation.** Advances in technology and the widespread adoption of digital platforms across the public and private sectors have accelerated the use of secure, interoperable digital identity documents.

Customer identity verification supports a broad set of use cases, including:

- Account origination/creation, particularly in banking and e-commerce, to confirm that individuals are who they claim to be and prevent identity fraud.
- Remote onboarding, which accelerates customer acquisition while avoiding the cost and friction of in-person verification.
- Prevention of fraudulent transactions and account takeovers following account creation.
- Protection against unauthorized account profile changes that could be used to bypass MFA.
- Age verification to ensure compliance with legal and regulatory requirements.
- Prevention of customer impersonation, particularly in call center interactions.

Third-party Identity Verification

Enterprises that rely on third parties and partners must protect their systems and sensitive data from unauthorized access. Identity verification helps control third-party risk by reducing the likelihood of compromise resulting from the misuse of partner or supplier identities.

Common third-party identity verification use cases include:

- Identity proofing before granting contractors or suppliers access to networks, applications, or sensitive information.
- Password resets and account recovery for third-party users.
- Delegated access assignment, ensuring that privileges are granted only to authorized individuals.
- Risk-based assurance enforcement, where verification requirements vary based on the level of risk and the nature of the relationship. For example, an external support team may require a lower level of assurance, while a delivery partner may require a higher level of identity verification.

Workforce Verification

Workforce identity verification helps protect enterprises against data compromise and identity fraud targeting employees. Historically, these efforts have focused on securing credential reset processes within IT support and help desks. However, significant gaps persist in the enterprise. Many organizations lack sufficient controls, leaving them vulnerable to social engineering attacks aimed at compromising high-value internal credentials. The risk has been underscored

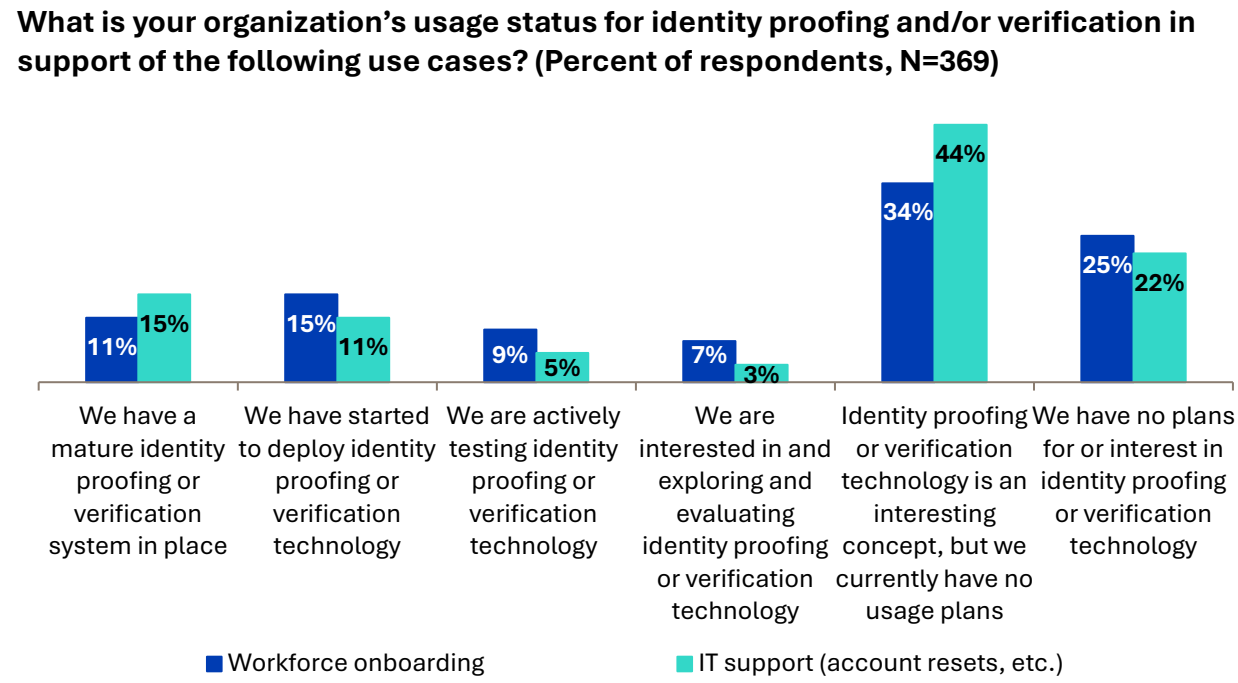
by a revised alert from the FBI, the US Cybersecurity and Infrastructure Security Agency (CISA), and international partners warning about Scattered Spider threat actors targeting support and help desk operations.

Beyond credential resets, workforce identity verification supports include a range of additional use cases, including employee onboarding, re-authentication and login, IT call center fraud prevention, account recovery, delegated access assignment, and other high-risk interactions.

An emerging attack vector is job candidate fraud, which differs fundamentally from credential reset threats. Job candidates are not yet provisioned in internal HR or IT systems, yet their identities must still be verified during the hiring process. Verifying candidate identities during the hiring process helps prevent wasted recruiting resources and reduces the risk of impostors gaining employment and subsequent access to sensitive enterprise systems.

Research from Enterprise Strategy Group (now Omdia) shows that only 26% of organizations currently have an identity proofing or verification system in place or being deployed. However, more than 50% report that they are either testing or considering such solutions.[2]

Figure 2: Workforce Identity Proofing Verification Implementation



Source: Omdia

[2] Source: Enterprise Strategy Group (now Omdia) Research Report, *Identity Security at a Crossroads: Balancing Stability, Agility, and Security*, September 2025.

The rise of generative AI, synthetic identities, and deepfakes represents a serious and growing risk. Deepfakes have already been used to carry out identity fraud. In 2024, a finance employee at a multinational company was deceived into transferring $25 million after participating in a deepfake video call in which fraudsters convincingly impersonated the company's CFO and other senior executives. As AI capabilities continue to advance and adversaries become more sophisticated and adept at exploiting this technology, the use of deepfakes for fraud will increase.

Covering All Use Cases: Enterprise Solutions for Identity Verification

Identity verification use cases are diverse and often span multiple teams within an enterprise, each with distinct objectives and risk tolerances. For example, customer-facing teams may prioritize reducing identity fraud losses while minimizing customer friction to get more "good" customers in the door. In contrast, cybersecurity teams may focus on preventing credential compromise that could lead to data breaches, even if doing so introduces additional friction for employees.

To be effective, enterprises must avoid siloed identity verification strategies that optimize for individual teams but leave the organization exposed in aggregate. Strong identity verification in a single application or business unit is valuable, but gaps in other areas can introduce significant risk. Siloed approaches often arise from organizational dynamics, as departments hesitate to collaborate out of concern that coordination may slow deployments or impact budgets. These blind spots are especially common in customer-facing processes and internal help desk operations, which frequently lack sufficiently rigorous controls against identity-based threats.

The Advent of Identity Threat Detection and Risk Mitigation

Effectively countering the threat posed by fraudulent identities requires a holistic approach that can be orchestrated across different enterprise workflows, including customers, third parties, and the workforce, and that can adapt to evolving identity attack patterns.

A holistic approach also enables enterprises to better understand and counter broader patterns of identity fraud. Organizations must ensure they see the full landscape of identity threats rather than isolated incidents. Focusing identity verification on a single application or a small set of use cases can obscure larger identity fraud patterns that span multiple systems and business units.

While deploying multiple identity verification methods in a sequential or "waterfall" model using specialized vendors for biometrics, document verification, or telecom-based verification

can reduce identity fraud, it can also introduce operational complexity and increased cost. Organizations must determine the optimal balance between single platform and multi-vendor approaches to achieve desired outcomes at the lowest total cost.

Modern identity threat detection and risk mitigation solutions combine a variety of adaptive identity verification methods, behavioral analytics, device and credential intelligence, and risk scoring. Together, these capabilities proactively detect and prevent identity-driven fraud while reducing overall risk exposure. As a result, organizations can stop identity-based attacks, protect revenue, meet regulatory requirements, and accelerate Zero Trust adoption.

To achieve optimal outcomes, enterprises should evaluate identity threat detection and risk mitigation solutions based on the following key capabilities.

Orchestration

Orchestration refers to the automated coordination and management of identity verification components across enterprise systems and processes. It leverages a broad library of authoritative identity data sources and risk signals that can be connected through a workflow builder interface. These workflows enforce policies and drive decisions related to identity verification and risk mitigation.

Effective orchestration enables dynamic, multi-layered risk decisions that adapt to evolving threats and align with an organization's risk tolerance. It typically includes feedback loops that validate confirmed fraud incidents and continuously refine policies. These loops may be powered by built-in analytics, reporting, or AI- and machine learning-based identity fraud forensics.

Enterprises must be able to apply identity verification consistently across workflows such as account onboarding, KYC, authentication, and identity fraud mitigation. Solutions should augment existing investments by integrating with IAM systems, security information and event management platforms (SIEM), workforce case management tools, and other relevant enterprise systems. Workflows and associated verification methods must also be adaptable to industry-specific regulations and organizational risk profiles.

Service Resilience

Identity threat detection and risk mitigation solutions are typically delivered as SaaS platforms. Downtime can have significant business impact, particularly for customer-facing identity verification use cases. Enterprises must evaluate resilience across multiple dimensions.

Infrastructure Resilience

Infrastructure resilience is the ability of a system to withstand disruptions and recover quickly while maintaining functionality. This includes high availability and fault tolerance achieved through multi-availability zones or multi-region deployment, automation, and redundancy.

Data Resilience

Data replication enhances resiliency by maintaining multiple synchronized copies of data across locations. This ensures availability and rapid recovery in the event of hardware failures, cyberattacks, or disasters. Redundant data architectures minimize downtime and reduce the risk of data loss.

Identity Verification Method Resilience

Most legacy identity verification vendors rely on a single proprietary or third-party method to verify identity. When that method fails, the impact on business operations can be severe. For example, if a hotel chain's identity verification service experiences an outage, customers may be unable to book rooms or access loyalty accounts. This can result in lost revenue, increased fraud exposure, and customer churn.

Mitigating this risk requires backup mechanisms for each authoritative identity data source and risk signal used in the verification process. Advanced solutions support automatic failover to alternative services, ensuring uninterrupted operations. This level of resilience is only possible when the solution includes a comprehensive library of authoritative identity data sources and risk signals.

Privacy

Privacy regulations have become progressively more stringent. Addressing compliance and data residency requirements is a critical capability for any identity solution. Regulations such as the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other national and state laws require careful attention to system design, data collection, storage, and transmission.

Many conventional identity verification solutions retain personally identifiable information (PII) during the proofing process, creating compliance challenges for organizations subject to strict privacy regulations.

Advanced identity threat detection and risk mitigation solutions address these concerns with a "privacy by design" strategy that does not retain PII by default. Instead, they use privacy-preserving techniques such as metadata mapping and data hashing to correlate risk signals across transactions without exposing sensitive information. These solutions also provide flexibility, enabling organizations to access or transfer data when necessary to meet their specific operational or regulatory requirements.

Portfolio of Authoritative Identity Sources and Risk Signals

A portfolio approach to robust identity sources and risk signals provides a higher fidelity threat signal. By ingesting a broad range of authoritative identity data sources, proprietary and third-

party risk signals, and customer attributes, identity threat detection and risk mitigation solutions can normalize and contextualize data to verify identities and detect anomalies across attack vectors.

The broader the portfolio of identity data sources and risk signals, the lower the volume of false positives that need triaging and the higher the true positive rate in identifying both known and emerging threats. A unified platform that supports multiple use cases, authoritative identity data sources, and risk signals offers a more cost-effective and operationally efficient approach to mitigating identity- and account-related threats.

A comprehensive solution that integrates these capabilities provides the foundation for a robust and scalable identity threat detection and risk mitigation strategy.

Representative Vendor for Identity Threat Detection and Risk Mitigation

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

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

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 organization's policies.

The ID Dataweb approach differentiates itself on the following dimensions:

- **Risk detection and orchestration.** Provides dynamic, multi-layered risk orchestration to detect identity fraud and respond in real time.
- **Privacy preservation.** Does not retain any PII, preserving privacy and regulatory compliance while supporting identity fraud forensics.
- **Service resilience.** Includes backup mechanisms that maintains continuous operations even if any of the built-in primary identity verification methods fail.

- **Fraud and identity expertise.** Leverages highly trained identity fraud experts who continuously feed insights into the platform and provide ongoing guidance to customers.
- **Mitigation of synthetic identity fraud.** Uses data integrity processes to minimize the risk of synthetic or fake identities by continuously reanalyzing PII and deduplicating instances where a single user holds multiple accounts.

This holistic approach enables organizations to deploy a single solution that integrates across multiple enterprise use cases, including customers, third parties (e.g., contractors and suppliers), and workforce, while reducing complexity, cost, and risk.

Conclusion

Identity threats, both internal and external, are significant, evolving, and increasing in sophistication. Maintaining the status quo in identity verification exposes organizations to revenue loss from identity fraud, data breaches, reputational damage, and potential career risk for employees.

Enterprises face multiple identity verification use cases across departments and applications. Rather than relying on fragmented solutions for each scenario, organizations should adopt holistic approaches that scale across multiple use cases. This strategy improves operational efficiency, reduces costs, and strengthens overall security. A unified set of controls enables identity and fraud teams to deliver consistent, low-friction user experiences, optimize system performance, and meet compliance obligations effectively.

Appendix

Methodology

This white paper is based on an in-depth review of the market that includes the following:

- Analysis using Omdia's market forecasting data and Enterprise Strategy Group (now Omdia) end user survey data.
- Vendor interviews that include briefings on current solutions and future plans.
- Information obtained from industry events and user conferences.

Todd Thiemann, Principal Analyst, Cybersecurity
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer