

# Identity Threat Detection & Risk Mitigation

What enterprise buyers need to know before selecting a vendor, and the platform questions that separate strong programs from fragile ones.



Contents

- 01 The Wrong Question Is Costing You
- 02 The Problem has Outgrown the Point Solution
- 03 What the Right Platform Delivers for Every Stakeholder
- 04 An Evaluation Framework Built for How You Buy

01

# The Wrong Question is Costing You

# 01

## The Wrong Question

Most organizations tackling identity fraud and account-related threats start with the same question: “Which vendor should we choose?”

It’s a natural instinct—and one the buying environment actively reinforces. Vendors eagerly pitch the importance of individual product features. Analysts publish comparison grids that rank point solutions against one another. Procurement processes rely on feature checklists that reward specificity over strategy. And RFPs are designed to break problems into discrete, scoreable requirements.

That approach works well when you’re buying a discrete product. But **it’s the wrong lens** when the problem you’re trying to solve isn’t discrete.

Identity fraud doesn’t enter through a single channel, target a single user population, or exploit a single weakness. It spans an interconnected set of threats that demands end-to-end visibility and a coordinated response.

As a result, a buying process that evaluates tools in isolation—each judged on its own merits against its nearest competitor—misses what matters most: **whether those tools work together to defend against the full spectrum of identity-based threats, or whether the gaps between them become part of the attack surface.**

That’s the shift this guide is designed to help you make—from evaluating point solutions in isolation to building a full lifecycle identity defense that spans attack vectors across every user population and every stage of the identity journey.

What follows explains why full lifecycle identity defense requires a platform approach, what that platform must deliver for the stakeholders responsible for using, managing, and justifying the investment, and how to structure an evaluation that prioritizes platform strength over individual feature performance.



### The platform question:

*The question isn’t which vendor has the best identity threat detection capability. It’s whether a single platform can address the full, connected spectrum of threats across customers, third parties, and workforce—without leaving you to stitch together point products that each solve only one piece of the problem.*

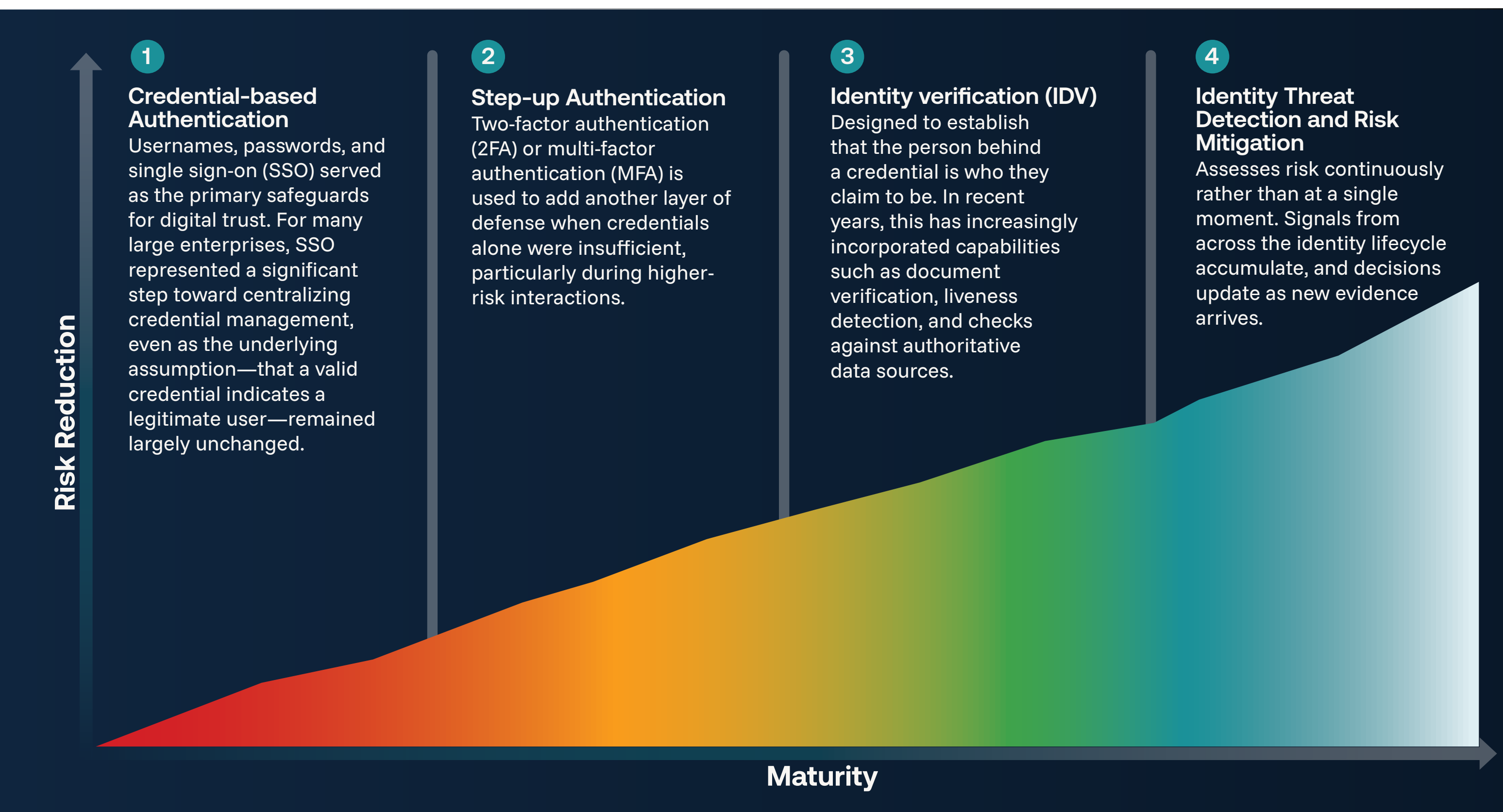


# 01

## From Credential Checking to Continuous Identity Threat Detection

*Identity verification has improved dramatically.  
So why isn't it enough?*

For much of the past decade, enterprise investment in identity protection has followed a predictable maturity curve. Organizations have progressed through three primary stages:



Each stage represents a meaningful improvement, driven by the same underlying imperative: reducing the risk and financial impact of identity-based attacks. As threat actors found ways around existing controls, organizations were forced to strengthen their defenses, not in pursuit of technological sophistication for its own sake, but because the costs of standing still continued to rise, including fraud losses, regulatory exposure, reputational damage, and account-related breaches.

Yet even robust IDV has a fundamental limitation: it is typically designed to answer an identity question at a particular moment in time. According to Omdia's identity verification maturity model<sup>1</sup>, IDV can validate an interaction using authoritative identity sources and risk signals, but by itself does not provide a continuous view of identity risk across digital activity. Threats such as account takeover, coordinated fraud, and synthetic identity abuse can emerge through patterns of behavior and signals that only become apparent across a broad range of interactions and over time.

A fourth—and more advanced—stage has emerged: what Omdia's maturity model defines as identity threat detection and risk mitigation. Rather than treating verification as a series of isolated decisions, this approach analyzes patterns across identities, credentials, devices, and interactions over time—creating a continuous feedback loop that enables risk decisions to evolve as new information emerges.

By bringing together adaptive identity verification, behavioral analytics, device and credential intelligence, and dynamic risk scoring, an identity threat detection and risk mitigation platform can extend protection across the enterprise's primary identity populations: customers, third parties, and the workforce.

That breadth changes the nature of the technology decision. The objective is no longer simply to determine whether an individual verification, authentication, or fraud-detection tool performs its specific function well. It is to establish a connected defense across the identity lifecycle—from onboarding and authentication through ongoing monitoring, re-verification, and deprovisioning—using authoritative identity data, risk intelligence, and customer-specific signals to inform decisions across every stage.

# 01

## Why Most Organizations Are Still Exposed

*If the maturity path is well understood, why do so many organizations remain vulnerable?*

Research conducted by CIO Dive's Studio, in partnership with ID Dataweb, surveyed 150 U.S.-based security and IT leaders across banking, financial services, insurance, and healthcare. While 82 percent of respondents recognize that identity is the new security perimeter, only 17 percent report being extremely confident in their ability to detect identity-based threats.

The gap between awareness and confidence is structural, not simply budgetary. The problem isn't a lack of tools or investment; it's fragmentation. Forty-three percent of respondents cited fragmented identity systems as their primary obstacle, while only 35 percent have explored continuous identity threat detection or risk scoring—even as 93 percent still rely on usernames and passwords as part of their access controls.

In practice, organizations have layered tools on top of tools, each designed to address a discrete problem without solving the underlying challenge of cohesion. The result isn't just a security gap. It's compounding technology debt: every additional point solution introduces more integration complexity, greater maintenance overhead, and another potential silo where identity intelligence can become trapped.

Fragmentation also creates a less visible problem: most organizations lack a comprehensive, real-time view of their identity threat posture. Instead, they rely on periodic audits, disconnected risk signals, and lagging indicators—sometimes discovering identity-based attacks only after a customer reports it or an incident has already occurred.

A platform approach changes that dynamic. By connecting identity activity, risk signals, and decisions across the identity lifecycle, it can provide continuous, empirical visibility into where threats are emerging and how risk is changing. Dashboards, analytics, and reporting then turn that visibility into actionable intelligence—giving security teams the information they need to intervene rather than simply reconstruct what happened after the fact.

The broader security market is moving in the same direction. The emergence of identity threat detection and risk mitigation reflects growing recognition that identity-based threats increasingly extend beyond the scope of traditional, point-in-time controls. Vendors across adjacent security categories—from privileged access management (PAM) to endpoint detection and response (EDR)—are expanding their identity-focused capabilities as identity becomes a more important dimension of enterprise attack detection and response.

## The State of Identity

# 82%

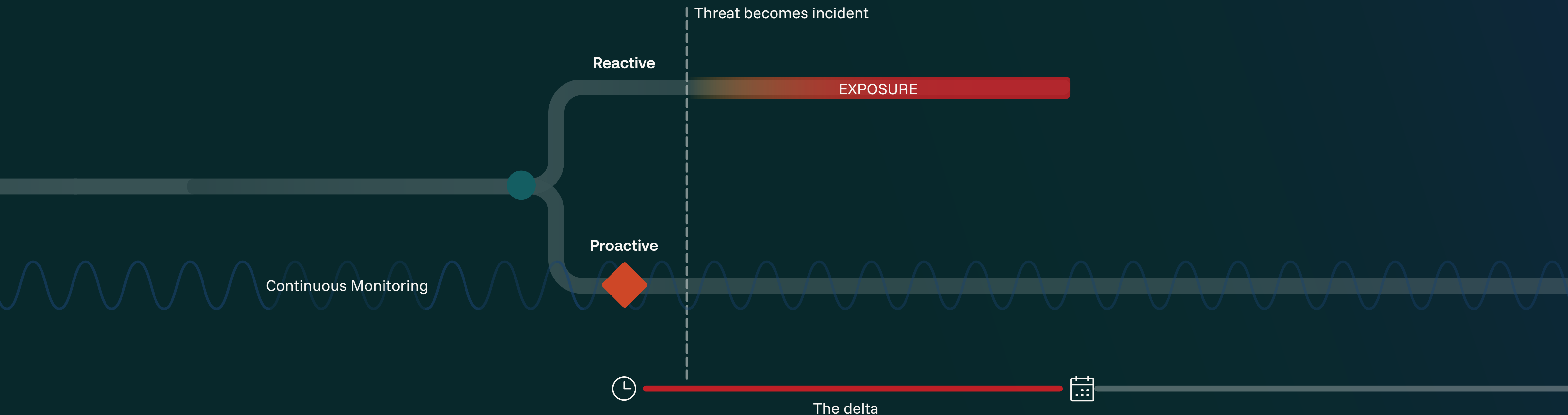
recognize that identity  
is the new security  
perimeter<sup>2</sup>

# 17%

extremely confident in  
their ability to detect  
identity-based threats<sup>2</sup>

# 43%

cite fragmented identity  
systems as their  
primary obstacle<sup>2</sup>



This convergence matters. When multiple segments of the security market move toward continuous identity threat detection, it signals a broader shift in how identity risk must be managed: from validating identity at individual moments to understanding and responding to risk continuously.

That shift ultimately comes down to posture: **reactive** or **proactive**.

A reactive approach waits for identity fraud to be reported, investigated, or confirmed before action is taken. By then, the consequences may already be material: accounts compromised, revenue lost, sensitive information exposed, or attackers moving on to their next target.

A proactive approach uses real-time risk signals and continuous intelligence to identify emerging threats and intervene earlier. This is where the market is heading. The organizations best positioned to respond will be those that move beyond damage control and build the visibility, intelligence, and orchestration required to prevent identity threats from becoming identity incidents.

02

# The Problem Has Outgrown the Point Solution

## The State of Identity

**\$25M**

transferred by a finance employee deceived by a deepfake CFO on a video call in 2024<sup>1</sup>

**23%**

report a strong understanding of AI-driven attacks<sup>2</sup>

**27%**

prioritize help desk interactions as a protection focus<sup>2</sup>

# 02

## AI Has Democratized Sophisticated Identity Fraud

The identity threat landscape has evolved in ways that expose a fundamental weakness in how most organizations have built their defenses.

What's changed isn't simply the volume of attacks. *It's their nature.*

Deepfakes, AI-generated documents, and AI-assisted social engineering are eroding many of the traditional signals that once helped security teams—and everyday users—recognize suspicious activity. Poor grammar, inconsistent tone, crude impersonation, and obvious visual artifacts are becoming less reliable indicators of identity-based attacks.

The consequences are no longer theoretical. In 2024, a finance employee at a multinational company was deceived into transferring approximately \$25 million after joining a video call in which fraudsters used deepfake technology to impersonate the company's CFO and other colleagues<sup>1</sup>. The incident illustrates what becomes possible as sophisticated impersonation technology becomes more accessible, convincing, and inexpensive to deploy at scale.

The CIO Dive's Studio survey, conducted in partnership with ID Dataweb, highlights a corresponding gap in organizational preparedness. While 90 percent of security leaders identify phishing as a top risk, only 23 percent report a strong understanding of AI-driven attacks, and just 27 percent prioritize help desk interactions as a protection focus<sup>2</sup>.

The result is a growing mismatch between how attackers establish trust and where organizations concentrate their defenses—leaving critical identity attack surfaces underprotected.

# 02

## Compromised Credentials Are Effectively Unlimited

At the same time, the widespread availability of compromised credentials has weakened another traditional indicator of trust: possession of a valid username and password. Credential stuffing and other forms of credential abuse allow attackers to approach authentication systems using information that legitimately belongs to the victim.

The scale of the broader problem continues to grow. In 2025<sup>3</sup>, losses reported to the FBI's Internet Crime Complaint Center reached approximately \$20.9 billion, underscoring the economic impact of increasingly scalable digital fraud and cybercrime.

The credential itself is no longer a reliable signal of legitimacy. An attacker using valid login information may initially appear indistinguishable from the legitimate account holder, allowing credential-based controls to be satisfied even when the person presenting those credentials is an impostor.

Effective detection therefore requires looking beyond the credential itself—evaluating behavioral patterns, device context, network intelligence, transaction activity, and other risk signals associated with the identity over time. The challenge is not simply collecting those signals but connecting them so that risk identified in one interaction can inform decisions elsewhere in the identity lifecycle.

Authentication data reinforces the broader point. Research cited by ID Dataweb found that 51 percent of organizations experience higher fraud rates when relying solely on usernames and passwords. By contrast, only 21 percent of organizations using facial biometric liveness detection as part of their approach report identity fraud attempts.

The takeaway is not simply that one verification method is stronger than another. **The method of verification matters, but so do the breadth, continuity, and integration of the controls surrounding it.**

# \$20.9B

losses reported to the FBI's Internet Crime Complaint Center, 2025<sup>3</sup>

# 02

## Identity Attacks Now Span the Entire Enterprise

### *Why isn't securing customer identities enough?*

Early identity verification efforts focused primarily on customer-facing fraud, particularly during account opening and eCommerce transactions. That narrow scope has left enterprises with significant blind spots elsewhere.

#### **Workforce identities are now primary targets.**

The rise of fraudulent job candidates has made clear that identity risk begins before employment. North Korean operatives<sup>4</sup>, for example, have used stolen and fabricated identities to obtain remote IT positions at U.S. companies, creating opportunities to generate revenue, access sensitive systems, and steal information. In 2024<sup>5</sup>, the U.S. Department of Justice indicted 14 North Korean nationals in a multiyear scheme that allegedly generated at least \$88 million through illicit remote IT work.

The implication extends beyond any single campaign: organizations need confidence in workforce identity before access is granted—and mechanisms to continuously evaluate that trust after it is established.

#### **Third-party and supply chain identities extend the attack surface**

Employees are not the only non-customer identities with access to enterprise systems and data. Contractors, partners, vendors, and other third parties may receive privileged or sensitive access while moving through identity processes and systems that differ from those governing the internal workforce.

That creates another potential blind spot. Customer-focused verification tools were not designed to establish and continuously evaluate trust across this extended population. As regulatory frameworks place greater emphasis on third-party risk, organizations increasingly need to understand not only which organizations they trust, but which individuals are acting on their behalf and whether that trust remains warranted.

#### **Help desk and IT support workflows are increasingly exploited**

Attackers are also targeting the processes designed to handle identity exceptions—password resets, MFA resets, account recovery, and emergency access—because these workflows can provide a path around otherwise effective security controls.

### **The Scope of the Problem:**

*Identity-based threats are not confined to a single team, system, or domain. They span customers, third parties, and the workforce, and surface across critical interactions—from account opening and authentication to profile changes, payment authorizations, and IT support requests. A platform that addresses only one of these areas provides only a partial view of identity risk. More critically, it limits the ability to connect signals across domains and detect the coordinated, multi-vector attack patterns that characterize the most damaging identity-based threats.*

Scattered Spider is a prominent example. The Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) have documented the group's use of social engineering to impersonate employees and convince IT help desks to reset passwords or MFA credentials, enabling attackers to gain access using seemingly legitimate credentials<sup>6</sup>.

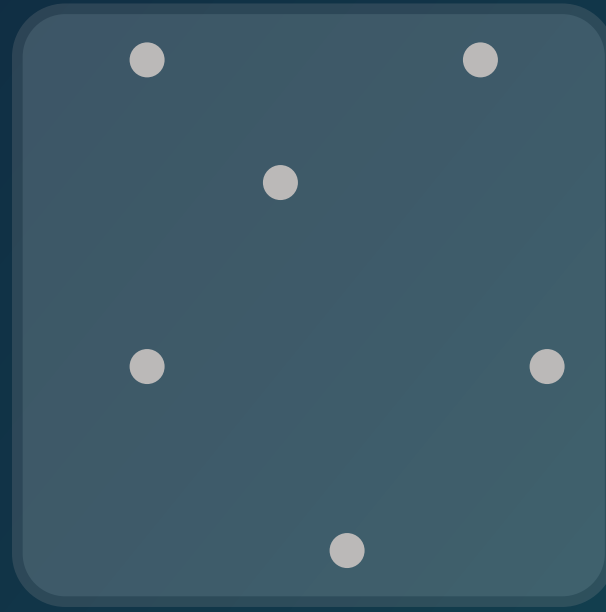
These workflows are particularly important because identity trust is being re-established at the very moment normal authentication mechanisms have failed or become unavailable. If the organization cannot reliably establish who is requesting the exception, the recovery process itself can become an attack vector.

Together, these threats expose the limitation of treating customer, workforce, and third-party identity as separate security problems. Attackers do not respect those organizational boundaries. They target whichever identity, interaction, or workflow offers the easiest path to trusted access.

## Siloed



Customer



Third Party



Workforce

## Connected



Customer

Third Party

Workforce

# 02

## Why Siloed Verification Creates Systemic Risk

*If deploying more tools is the natural response to a growing attack surface, why can it still leave organizations more vulnerable?*

As the attack surface expands, organizations often deploy specialized tools for each context: a biometric solution for customer onboarding, a workforce verification provider for employee identity, and a separate fraud analytics engine. Each may perform well within its domain. But no individual tool has visibility into the aggregate risk emerging across them.

Siloed approaches obscure the broader patterns of identity fraud that span systems, interactions, and business units. An attacker probing both a customer portal and a partner portal, for example, may generate activity that appears insignificant when viewed

independently. A unified platform can correlate those signals and evaluate them as part of a broader pattern of behavior.

That creates a fundamental problem: optimization at the team level can create vulnerability at the enterprise level. Individual controls may be effective, yet the organization can still lack the connective intelligence needed to understand how threats move across them.

The answer isn't to eliminate specialized capabilities—it's to connect them. As Omdia notes, a unified platform that integrates multiple use cases, authoritative identity data sources, and risk signals can

improve both cost and operational efficiency compared with a fragmented approach.

The goal isn't to replace what works. It's to ensure the gaps between tools don't become part of the attack surface.

# 02

## What the Right Platform Looks Like

*Does platform strength depend on individual capabilities—  
or how well they work together?*

The defining characteristic that separates an effective identity threat detection and risk mitigation platform from a collection of loosely integrated point solutions is that it is multi-layered. No single signal or detection method is sufficient on its own. An effective platform combines adaptive identity verification, behavioral analytics, device and credential intelligence, and dynamic risk scoring—each contributing a distinct dimension of risk intelligence. Together, those signals provide the context needed to make more confident decisions in ambiguous scenarios where any one signal may be inconclusive.

It must also be continuous. Identity risk does not begin and end at login, and neither can detection. An effective platform evaluates identity interactions across the full lifecycle—from onboarding and authentication through account activity, profile changes, re-verification, and deprovisioning—maintaining a dynamic risk profile that evolves as new signals and patterns emerge. This continuous visibility enables organizations to identify threats that develop gradually across multiple interactions rather than presenting as a single, obvious event.

Connecting these capabilities is orchestration. A workflow engine that brings identity data, risk signals, and policy-driven decision logic together enables organizations to adapt verification and response to the risk of each interaction. Just as importantly, orchestration provides the architectural flexibility to evolve as threats, technologies, and business requirements change. Signal sources and capabilities can be added or replaced without rebuilding the underlying decision framework—supporting extensibility, scalability, and consistent, auditable outcomes.

Finally—and most critically—the platform must be unified across customers, third parties, and the workforce. Unified coverage does more than extend protection to each identity population. It allows intelligence generated in one domain to inform decisions in another, providing visibility into patterns that would otherwise remain fragmented across separate systems.

**That is where the platform becomes more than the sum of its parts: not simply by combining capabilities, but by connecting signals, decisions, and identity activity across the enterprise.**

**Adaptive Identity  
Verification**

**Behavioral  
Analytics**

**Device and Credential  
Intelligence**

**Dynamic Risk  
Scoring**

**03**

# **What the Right Platform Delivers for Every Stakeholder**

# 03

## Key Decision-makers

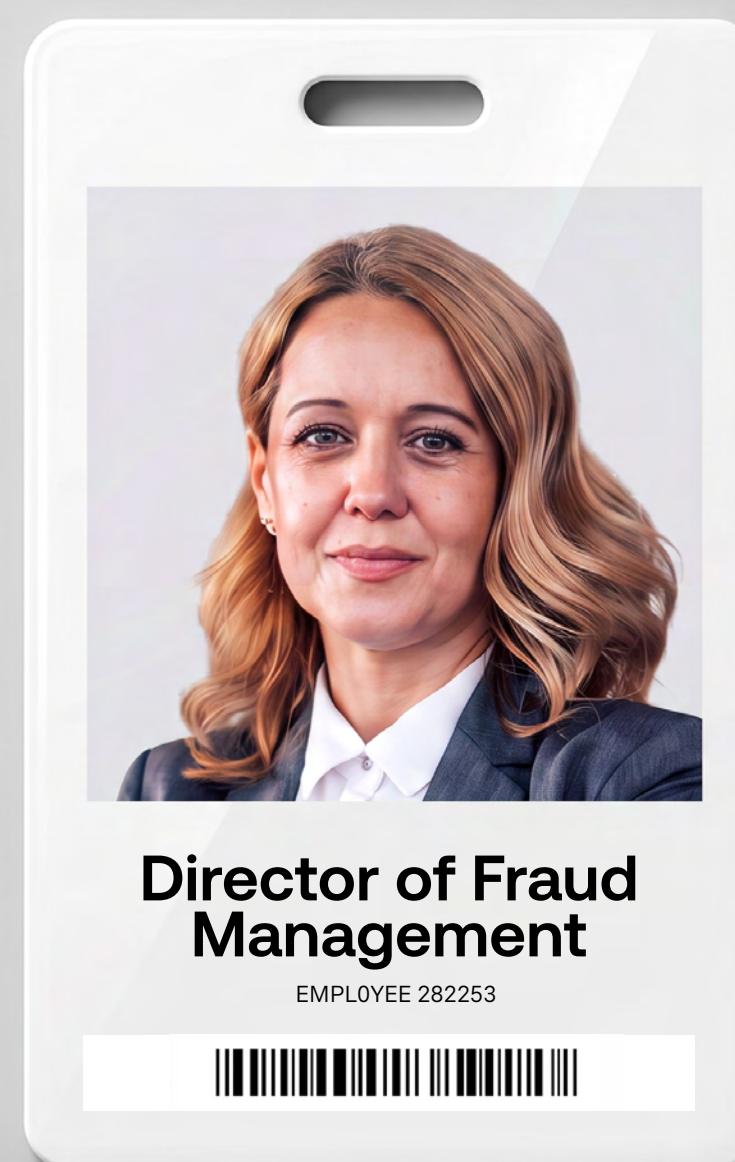
The decision to invest in identity threat detection and risk mitigation is rarely made by a single individual. Security leadership, fraud management, IT, compliance, product, business unit owners, and procurement each bring distinct priorities, success metrics, and risk tolerances to the evaluation. A strong platform must create value across that buying center.

This chapter examines the platform through the lens of three key decision-makers.

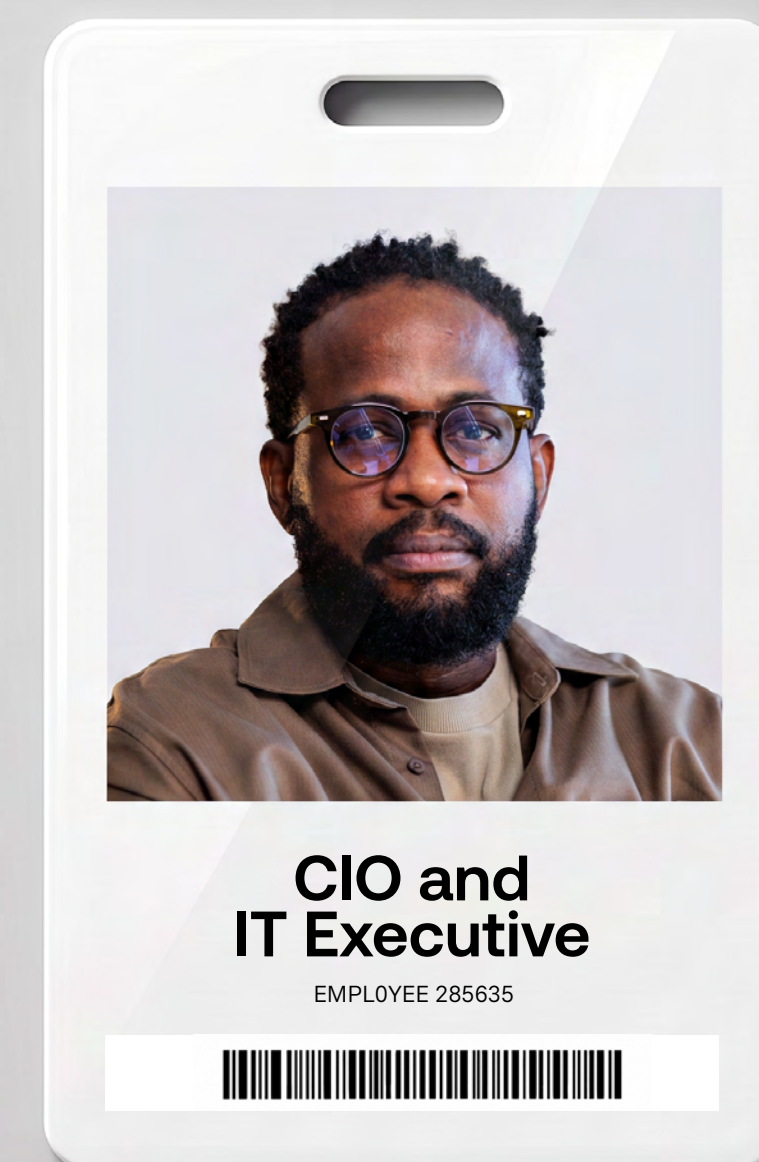
Each section examines what matters most to that stakeholder, where fragmented approaches fall short, and what an orchestration-based platform must deliver to close the gap.



**Focus:** Reducing enterprise identity risk and strengthening security posture.



**Focus:** Preventing identity fraud while improving decision accuracy and minimizing customer friction.



**Focus:** Integration, scalability, operational efficiency, and return on investment.

# 03

## The Security Executive

For most security executives, the challenge isn't a lack of security tools. It's that identity systems often make risk and policy decisions in isolation. Modern identity-based attacks cross channels, systems, and identity populations as attackers search for the weakest path to trusted access. Without shared risk intelligence and consistent decision-making across those environments, suspicious activity identified in one interaction may never inform access decisions in another.

Security executives therefore need visibility into identity risk across the enterprise—not just at login, but throughout the identity lifecycle. They need dynamic policy enforcement that can allow, challenge, or block interactions based on risk without imposing unnecessary friction on legitimate users. They need audit-ready reporting for regulators, insurers, and internal governance teams without extensive manual effort. And they need resilient infrastructure that avoids creating new points of failure as identity becomes increasingly central to the security architecture.

An orchestration-based platform brings those requirements together. Shared threat intelligence across customers, third parties, and the workforce provides broader visibility into risks that might otherwise remain isolated within individual systems. Adaptive policy enforcement creates a consistent decision framework that can scale across identity populations and use cases. Continuous feedback enables risk models and policies to evolve as new threats emerge, while privacy-conscious architecture can support the correlation of risk signals without unnecessarily exposing sensitive identity data.

Together, these capabilities give security leaders the visibility, policy control, and adaptability required to operationalize a stronger Zero Trust strategy.



### How Success Is Measured

- Reduction in successful account takeover and identity-related fraud.
- Identity threats detected and contained.
- Mean time to detect and remediate identity threats.
- Audit pass rates and compliance findings.
- Reduction in manual effort through automated verification and policy enforcement.

# 03

## The Director of Fraud Management

For fraud leaders, the objective isn't simply to detect more suspicious activity. It's to distinguish genuine identity fraud from legitimate behavior with greater accuracy.

False positives make that challenge particularly costly. Legitimate users incorrectly flagged by blunt detection systems create customer friction, increase support costs, and consume analyst capacity that could otherwise be directed toward genuine threats. At the same time, sophisticated attackers increasingly combine synthetic identities, compromised credentials, AI-generated artifacts, and coordinated behaviors designed to appear legitimate when individual signals are evaluated in isolation.

Fraud leaders therefore need higher-confidence decisions with fewer false positives. That requires a broad set of authoritative identity data, proprietary and third-party risk signals, behavioral intelligence, and customer-specific attributes that can be evaluated together rather than independently. It requires analytics capable of identifying patterns that static rules may miss, coupled with policies that can be tuned as fraud patterns evolve. And it requires real-time dashboards and reporting that give fraud teams visibility into emerging threats without manually assembling data from disconnected systems.

An orchestration-based platform provides the connective layer. Multiple risk signals add context to each interaction, enabling more informed decisions when any individual signal is inconclusive. Continuous re-evaluation can also identify changes in risk after initial verification—for example, changes in phone intelligence, identity attributes, or other indicators that warrant renewed scrutiny.

The same principle can be applied proactively. Evaluating identity populations before an interactive event can surface potentially high-risk identities before they reach a transaction or authentication workflow. Resilient workflows can also route decisions through alternative signals or verification methods when an individual data source or capability is unavailable.

Combined, these capabilities move identity fraud management away from a sequence of isolated checks and toward a continuously informed risk model—one that can adapt as identities, behaviors, and attack methods change.



### How Success Is Measured

- Reduction in account takeover, synthetic identity fraud, and fraud losses.
- False-positive and false-negative rates.
- Mean time to detect and remediate fraud.
- Verification automation rates and analyst hours saved.
- Customer friction and abandonment rates.

# 03

## The CIO and IT Executive

For CIOs and IT leaders, identity fragmentation creates a different problem: complexity compounds.

Disconnected identity and access management (IAM), identity verification, identity fraud, and risk systems introduce integration requirements, technical debt, and operational overhead with every additional tool. Legacy environments can make those integrations even more difficult and expensive to maintain. Meanwhile, cloud migration, API-first architectures, workforce transformation, and expanding partner ecosystems require identity infrastructure that can scale without creating another layer of complexity.

CIOs therefore need an architecture that can integrate with existing IAM systems, SIEM platforms, case management tools, and business applications without requiring wholesale replacement of current infrastructure. The platform should augment existing investments while providing the flexibility to add, replace, and orchestrate capabilities as requirements change. It must scale reliably to enterprise volumes while providing analytics that make identity risk visible to both operational teams and executive leadership.

This is also where the economic case for orchestration becomes important. Consolidating identity workflows through a common platform can reduce duplicate integrations, simplify vendor management, lower maintenance requirements, and decrease the manual effort required to reconcile information across systems. A shared source of identity risk intelligence can also accelerate investigation, incident response, and compliance reporting.

For the CIO, the value of the platform is therefore not simply consolidation. It is architectural leverage: the ability to extract more value from existing identity investments while reducing the complexity required to connect, operate, and evolve them.

That creates a clearer return on investment (ROI) narrative built around measurable outcomes such as reduced integration and operating costs, lower fraud losses, decreased manual effort, faster identity decisions, and improved operational resilience.



## How Success Is Measured

- Reduction in identity technology and integration costs.
- Reduction in manual verification and administrative effort.
- Onboarding completion rates and time-to-verify.
- Platform availability and operational resilience.
- Audit success rates and compliance findings.
- Percentage of identity workflows managed through a common orchestration layer.

04

# An Evaluation Framework Built for How You Buy

# 04

## How to Use the Framework



When organizations evaluate identity threat detection and risk mitigation platforms, they often start by assembling a list of features. That instinct isn't entirely wrong—capabilities matter. But feature lists tend to evaluate capabilities in isolation, making it easy for vendors to claim parity by checking the same boxes without demonstrating the architecture required to make those capabilities work together.

The framework in this chapter is designed to shift the evaluation from feature presence to platform strength. It focuses on the capability areas that distinguish a truly unified platform from a loosely integrated collection of tools. For each, it identifies the questions buyers should ask, what strong answers should demonstrate, and why those distinctions matter in practice.

Use the framework to structure RFIs and RFPs, guide proof-of-concept design, and anchor procurement conversations around the architectural capabilities that ultimately determine the platform's effectiveness, adaptability, and long-term value.

04

How to Use the Framework

| Capability Area                                    | Questions to Ask Any Vendor                                                                                                                                                                                                                                                                                                                                                                                                              | Why It Matters                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Risk Orchestration                                 | Can you demonstrate a workflow that combines multiple authoritative identity sources and risk signals into a single, policy-driven decision? Can policies dynamically allow, challenge, route, or block an interaction based on changing risk? How are decisions and the signals behind them carried across workflows?                                                                                                                   | Orchestration is what turns individual capabilities into a coordinated defense. Without a shared decision layer, signals may remain isolated and policies become harder to apply consistently across identity interactions.                                                                           |
| Coverage Across Identity Populations and Lifecycle | Does the same platform support customers, third parties, and workforce identities? Demonstrate how it handles use cases across the lifecycle, including account opening, authentication, account recovery, help desk verification, ongoing monitoring, and deprovisioning. Can risk identified in one workflow inform decisions in another?                                                                                              | Identity threats cross populations, systems, and lifecycle stages. Breadth matters, but connected breadth matters more: the platform should be able to carry intelligence across interactions rather than simply support multiple use cases independently.                                            |
| Breadth of Identity and Risk Intelligence          | What categories of signals can be evaluated in a single decision—including identity, risk, possession, device, network, credential, and behavioral intelligence? Can multiple checks execute in parallel? Which data sources are native to the platform, which are integrated, and which must we procure separately? Are results normalized into a common decision framework and report? Can we incorporate our own data and attributes? | No individual signal provides sufficient context for every identity decision. Layering independent signals allows one source to corroborate, challenge, or add context to another. Breadth also creates options for alternate decision paths when individual signals are unavailable or inconclusive. |
| Service Resilience and Fallback                    | What happens when a primary authoritative identity data source or verification method becomes unavailable? Can workflows automatically route to alternative sources or methods? Which dependencies have fallback coverage? What availability commitments and SLAs do you provide, and how are third-party dependencies accounted for?                                                                                                    | Identity infrastructure can sit directly in critical customer and workforce journeys. A dependency failure should not automatically become a failed identity decision or blocked user journey. Resilient architecture provides alternative paths when individual components become unavailable.       |

04

How to Use the Framework

| Capability Area                               | Questions to Ask Any Vendor                                                                                                                                                                                                                                                                                                                                                     | Why It Matters                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Privacy, Security, and Data Residency         | What PII does the platform collect, process, retain, and transmit? What is retained by default, for how long, and where? How is identity activity correlated when sensitive data is minimized or tokenized? What residency, deletion, encryption, and access-control options are available? In the event of a breach, what customer and user data could potentially be exposed? | Identity platforms process particularly sensitive information, making data architecture part of the security evaluation itself. Buyers should understand whether the platform minimizes sensitive data while preserving enough context for detection, investigation, and audit requirements.                                                                                                                                                                             |
| Policy Granularity and Precision              | What underlying signals can policies act on? Can administrators build logic using individual attributes and contextual signals, or only vendor-generated aggregate scores? Can policies combine multiple signals, apply different thresholds by use case, and explain why a decision was made?                                                                                  | Aggregate scores simplify decisions but can obscure the factors driving them. Granular policy controls allow organizations to incorporate business context, tune responses more precisely, and better balance identity fraud prevention against customer friction.                                                                                                                                                                                                       |
| Integration and Time to Value                 | What does integration with our IAM, SIEM, fraud, and case management environment require? How many APIs or integration points are needed for a typical deployment? What can be configured without custom development? What is the typical implementation timeline, and what ongoing resources will our team need?                                                               | Integration complexity directly affects deployment time, operating cost, and technical debt. A platform should augment existing infrastructure rather than force unnecessary replacement, while minimizing the number of integrations the organization must build and maintain. API-first, low-code platforms designed to augment existing infrastructure deliver faster value and lower implementation risk. Look for a single API architecture to ensure efficiencies. |
| Reporting, Analytics, and Compliance Evidence | Can we view identity activity and risk across populations and workflows through centralized reporting? What dashboards are available out of the box? Can we drill from an aggregate trend into the signals and decisions behind individual events? What evidence can be exported for audits and investigations? What self-service analytics are available?                      | Centralized, normalized reporting turns activity across individual workflows into enterprise-level identity intelligence. Without it, teams may be able to investigate individual events while still missing trends that emerge across populations, channels, or time.                                                                                                                                                                                                   |

04

How to Use the Framework

| Capability Area                                   | Questions to Ask Any Vendor                                                                                                                                                                                                                                                                                     | Why It Matters                                                                                                                                                                                                                                                                                                       |
|---------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Continuous Re-evaluation and Population Screening | Does risk evaluation occur only during interactive identity events, or can existing identities be re-evaluated over time? What changes can trigger renewed evaluation? Can existing populations be screened in batch to identify emerging risk? How are new findings incorporated into future policy decisions? | Identity risk changes after initial verification. Attributes, credentials, devices, and other risk indicators can change over time, while previously established identities may later warrant additional scrutiny. Continuous and scheduled evaluation helps close the gap between point-in-time identity decisions. |

# 04

## Designing the Proof of Concept



### Coordinated attack spanning domains

Suspicious activity begins in a customer portal and is followed by a related workforce or third-party access attempt.

**Does intelligence from one interaction inform decisions in the other?**



### Risk that emerges over time

An identity successfully passes onboarding but accumulates anomalous signals in subsequent interactions.

**Does the platform recognize the changing risk profile and adapt its response?**



### High-risk help desk interaction

An emergency access or account recovery request exhibits indicators of social engineering.

**Can the platform combine identity, device, behavioral, and contextual signals to determine the appropriate response?**



### Critical dependency failure

A primary verification method or data source becomes unavailable during a high-risk interaction.

**Does the workflow fail, stop the user journey, or automatically invoke an appropriate alternative?**

If a proof of concept (POC) is part of your vendor selection process, consider what the POC is actually designed to prove. Traditional POCs often validate individual features in isolation. That may tell you whether those features work, but it won't necessarily tell you whether the platform works as a whole.

Thus, design the POC to test architectural integrity: whether signals, policies, workflows, and decisions remain connected as identity risk moves across systems, populations, and time.

Build scenarios that require multiple capabilities to work together, rather than testing single-system performance.

These example scenarios test something a feature demonstration cannot: whether the platform can turn multiple capabilities into a coherent identity defense. Look for consistent policy execution, transparent decision logic, cross-workflow intelligence, graceful fallback, and auditable outcomes.

# 04

## The Procurement Conversation Worth Having

Technical capability is only part of the evaluation. Three considerations that may receive too little attention in a standard RFP can have a significant impact on long-term platform value:

### 1. Identity fraud expertise

Ask what expertise sits behind the technology. Does the vendor employ identity fraud specialists who analyze emerging attack patterns? How are those insights incorporated into risk intelligence, policies, or detection capabilities? How quickly can the vendor help your team understand and respond when a new attack method emerges?

The question isn't simply whether human expertise exists. It's how effectively that expertise improves the platform and supports your team.

### 2. Adaptability to regulatory and threat change

Identity requirements will continue to evolve alongside regulations, attack methods, and technology. Ask how quickly policies, workflows, data sources, and verification methods can be changed—and which changes require vendor support or custom engineering.

A platform designed for adaptability gives organizations greater freedom to respond as requirements change without repeatedly rebuilding the underlying identity architecture.

### 3. Total cost of ownership

License cost is only one component of TCO. Integration and maintenance requirements, internal staffing, third-party data costs, manual review, false-positive management, service disruption, and the cost of changing capabilities over time can all materially affect the economics of a platform.

Ask vendors to quantify these costs—not simply the price of their technology. The relevant comparison is the **total cost of operating the identity defense, not the price of an individual feature.**

## A final note on platform versus feature competition:

Vendors in this category may offer many of the same individual capabilities. The more meaningful distinction is what happens between them: how signals are connected, how decisions are orchestrated, how risk intelligence carries across interactions, and how the architecture adapts when threats, dependencies, and requirements change.

**That is where platform strength becomes visible.**

Demand live demonstrations. Design the proof of concept if required to stress the architecture, not simply validate the features. Test what happens across systems, across identity populations, over time, and when individual components fail.

**That's where the differences become clear—and where long-term platform value is determined.**

# Sources

1. [Controlling Identity Risk: Detecting and Mitigating Identity Threats, Omdia, January 2026](#)
2. [The State of Identity: How Organizations Are Bridging the Confidence Gap, CIO Dive's Studio, February 2026](#)
3. [2025 IC3 Annual Report, Federal Bureau of Investigation Internet Crime Complaint Center \(IC3\), 2025](#)
4. [Mandiant, North Korean IT Worker Fraud Campaign, 2024](#)
5. [U.S. Department of Justice, press archives](#)
6. [FBI and U.S. Cybersecurity and Infrastructure Security Agency \(CISA\), Joint Advisory on Scattered Spider, 2023](#)



ID Dataweb™ delivers identity threat detection and risk mitigation solutions to safeguard against identity fraud and account-related threats, all without disrupting the user experience.

[Book a demo](#)



[iddataweb.com](https://iddataweb.com)

ID Dataweb, Inc.  
5875 Trinity Parkway  
Suite 110  
Centreville, VA 20120  
United States