

Identity Integrity

Solution Brief

Corroborate an individual's identity in minutes — flag inconsistencies, surface risks, and know where to focus before you make a critical decision.

THE PROBLEM

Your tools verify the document. But is the person real?

Identity integrity is the new firewall. Distributed workforces, remote hiring, and AI-enabled fraud have made one question — “is this person who they claim to be?” — among the most consequential an organization can ask, and one of the hardest to answer.

Traditional identity verification checks whether a document is legitimate. Background checks confirm records against databases. But neither answers the deeper question: **does this individual's provided information hold up when cross-referenced across truly independent sources?**

Synthetic identities, AI-generated credentials, and nation-state-affiliated infiltration schemes are getting past document-based checks — because while the documents themselves may be real, the person behind them isn't. And this isn't just a hiring problem: when an insider threat investigation raises questions about an employee, or a security event demands assurance across sensitive roles, the same question applies.

THE THREAT IS REAL, AND GROWING

25%

of candidate profiles estimated to be fake by 2030
(Gartner)

\$19.5 million

average cost of insider risks per organization
(Ponemon)

50–200%

of salary — the cost of a bad hire
(SHRM)

THE SOLUTION

Corroborate identity across sources that can't be faked

Identity Integrity is a client-led, on-demand assessment in the Ascend™ platform that cross-references an individual's provided information against multiple independent sources — breach data, investigation databases, official public records, and digital footprint analysis — to assess whether the person behind the documents is consistent, traceable, and real.

It requires nothing from the individual — no selfie, no document upload, no added steps. Your team runs the report using information you already have. In minutes, you get a clear identity integrity assessment, the specific signals behind it, and the underlying evidence — so you can decide whether to proceed, investigate further, or escalate.



USE CASES

One capability, applied across the workforce lifecycle



PRE-HIRE SCREENING

Corroborate a candidate's identity early — before significant interview and onboarding investment. Flag synthetic identities and fabrication to focus scrutiny where it matters.



EMPLOYEE INVESTIGATION

When your monitoring raises flags or questions arise about an existing employee, run a report to quickly determine whether further investigation is required.



IDENTITY ASSURANCE AT SCALE

Following a security event, screen sensitive roles or broader populations via API to surface inconsistencies that warrant review.

The screenshot displays a user profile for David [redacted] with a creation date of 2:13pm July 21 2025. The interface includes tabs for Overview, Job History, Breach Data, Digital Footprint, and Personal Details. The 'Flagged Signals' section lists several alerts:

- VoIP detected for provided phone number +1 (212) 684- [redacted]
- Breach records do not match provided information
- Digital footprint is less than a year old

The 'Source Overview' section provides an overview of exact matches between provided information and available data sources. A table below compares the 'Investigation Database' with 'Provided LinkedIn' data:

Sources	Name	Email	Phone	Address	Notes
Investigation Database	✓	✓	✓	✗	
Provided LinkedIn	✓	✓	✓	✗	



THE VALUE

Know who you're dealing with — before it matters most

- ✓ **Confidence before you commit**
Know whether an individual's information holds up before you hire or grant access
- ✓ **Clear prioritization**
An overall identity discrepancy score tells your team where to focus and what to escalate
- ✓ **Less time wasted**
Interview and employ people who are who they claim to be
- ✓ **Insights in minutes, not days**
Risk-based identity assessment at the speed of your process
- ✓ **Catch what other tools miss**
Flag synthetic and misrepresented identities before they gain or retain trusted access
- ✓ **Assurance across the workforce lifecycle**
Protecting IP, critical systems, and reputation

WHY NISOS

We corroborate what can't be faked

OSINT-based corroboration, not document verification. Documents can be forged or stolen. Breach history, long-established accounts, and historical records can't be fabricated retroactively. It's not a replacement for your IDV; it's the layer that catches what document verification misses.

Breach data as a signal. Breaches are so common that an experienced professional who appears in no breach data may signal a synthetic or fabricated identity — a flag no traditional check would surface.

Zero friction. No selfie, no document upload. Because this is not a background check, no authorization is required from the individual. Your team runs the report using information you already have.

Risk signals, not decisions. Identity Integrity flags risk and surfaces the signals behind it, so your team can decide how to act with confidence. Not a background check, not a consumer report.

Part of an integrated suite. Identity Integrity works alongside the Ascend Insider Threat module, and when it surfaces significant concerns, findings are structured for easy escalation to a deeper investigation — with your own team or ours.

TAKE ACTION TODAY

Know who you're dealing with — before it matters most.

Corroborate identity in minutes. Flag what others miss. Focus your team where it counts.

Contact us at info@nisos.com • nisos.com/contact/