GetReal

CASE STUDY

Securing the Talent Acquisition Supply Chain At A Top-5 U.S. Staffing Firm

The Talent Acquisition Supply Chain Security Challenge

As large organizations increasingly rely on a distributed network of recruitment partners, the integrity of the talent supply chain has become a critical component of enterprise security and attack surface management given the dramatic increase in AI-powered deepfakes and human imposter attacks, particularly by the DPRK and China.

Chief Information Security Officers (CISOs) have increasingly expressed the need to secure not only internal recruiting processes but also all external "inputs" into their talent acquisition programs. This includes candidates sourced through RPOs, staffing firms, and other third-party providers.

GetReal addresses emerging security risks within modern talent acquisition ecosystems. We provide a cost-effective, programmatic approach for GetReal's enterprise customers to enforce consistency of security standards in their talent acquisition supply chain partners and ensure their own security risk posture is not impacted by supply chain attacks.

Why the Talent Supply Chain Is Being Targeted

Most Global 2000 organizations operate with a primary, centralized Recruitment Process Outsourcing (RPO) provider, supplemented by two to three additional partners to support specialized, regional, or high-volume hiring needs. In many cases, these RPO providers further extend their capabilities through subcontractors or niche solution providers. This highly interconnected model creates a complex "human capital supply chain," where multiple third parties contribute candidates into an organization's hiring pipeline. While this structure enables scale and flexibility, it also introduces significant variability in security practices across providers that can change the enterprise risk profile for their downstream customers.

Numerous recent incidents of RPO providers unknowingly placing W-2 employees who were later identified as threat actors have highlighted the risks inherent in this model. These campaigns often involve sophisticated fake candidate profiles that closely resemble legitimate applicants, making detection difficult and exposing downstream organizations to material risk. It has also highlighted the fact that nation-state adversaries are increasingly targeting RPOs given their lack of historical security controls in the talent acquisition process beyond traditional background checks.

Key challenges driving the need for layered security include:

- Inconsistent security controls across RPOs, subcontractors, and niche providers
- Lack of standardized verification processes for candidate identity and authenticity
- Limited visibility into third-party recruiting pipelines
- Absence of compensating controls to detect and mitigate fraudulent candidate activity
- Increased attack surface, mirroring risks seen in software supply chain attacks

As a result, organizations face growing exposure to insider threats originating from their extended talent ecosystem.

Inside a Top-5 U.S. Staffing Firm's Response

One of the five largest staffing firms in the U.S., which places up to 50,000 roles annually for Fortune 1000 clients across IT, healthcare, engineering, and finance, sits at exactly the point in the talent acquisition supply chain that adversaries now target. Facing an emerging DPRK threat, the firm moved proactively to verify its remote workforce. GetReal verified 60 remote workers in days, protected a $2 million client contract, and saved an estimated $250,000 in travel costs and lost productivity.

The Problem

When a Fortune 1000 company hires through a staffing firm, it is outsourcing a security decision. The client trusts that firm's vetting process to stand as a line of defense between its systems and deceptive candidates, fraudsters, and sanctioned individuals, entities, and countries. For a firm placing talent at this scale, that trust is the product.

North Korean operatives using fabricated or stolen identities — credentials engineered to pass conventional background checks — have systematically targeted remote IT roles placed through staffing firms. With strong English skills, deep technology fluency, and coordinated deception playbooks, these actors represent precisely the kind of supply-chain infiltration that bypasses traditional controls.

60

employees remotely verified in less than a week

$2M+

client contract protected

$250k+

in estimated travel costs and lost productivity saved

This firm had relied on video interviews, background checks, and manual comparisons of government IDs to video interview screenshots as early warning signals. Those controls depended on human intuition, were inconsistently applied, and were exactly what these nation-state campaigns were designed to defeat. As awareness of the North Korea IT threat and other forms of candidate fraud grew, the firm's clients and prospects began asking harder questions — and demanding auditable answers.

The Turning Point

Major enterprise clients, including Fortune 100 accounts, began requiring evidence that their staffing partners had controls in place to detect and stop nation-state infiltration across recruiting, hiring, and business process outsourcing. A documented process was no longer enough. Manual, judgement-based vetting could not produce the auditable proof these downstream organizations now expected from every input into their talent acquisition programs.

The firm's CISO, general counsel, and head of workforce integrity collaborated to identify a partner and design a program for consistent, thorough verification — both of new candidates and of the authenticity of recently placed workers.

The Response

The firm engaged GetReal Security for its multimodal deepfake detection and identity assurance technology to revalidate its placed remote workforce and produce the documented attestation its clients required. GetReal's Continuous Identity Verification Platform evaluated interactions with the remote workforce seamlessly, without disrupting workflows or signaling to workers that they were under review.

Within days, a four-person team had revalidated 60 employees. The platform analyzed interactions with each worker to flag AI-generated manipulation, including face swaps, voice manipulation, and AI avatars. Detection grounded in forensic science with explainable evidence produced results the client could trust and defend, rather than vague, black-box confidence scores.

In situations involving higher-risk candidates and workers, GetReal forensics and threat intelligence experts conducted deeper investigations — analyzing audio and video streams, profile images, and additional telemetry to confirm the authenticity of each worker's identity. Competitors train on yesterday's data and tools, then fail against new attacks or produce low-accuracy guesses. GetReal grounds detection in forensic science with explainable evidence, so results are trustworthy and client-defensible, not opaque confidence scores.

The Results

The result was auditable verification of placed workers' identities that stood up to client, legal, and regulatory scrutiny. It became the foundation of a workforce integrity program the firm could present to clients with confidence — a compensating control where none had existed before.

For a firm placing 50,000 people a year, the ability to verify workforce integrity quickly, and to prove it to clients and prospects, is now a competitive advantage rather than a liability in the talent acquisition supply chain.

© GetReal Security