imper.ai

CASE STUDY

How a leading technology company uses imper.ai to prevent DPRK from infiltrating the workforce.

INDUSTRY	WORKFORCE	ATS	RESULT
Technology	**3,000+**	**Greenhouse**	**4 Blocked. Zero Access.**

The organization recruits globally for remote software engineering and infrastructure roles. Its hiring pipeline runs through Greenhouse and conducts technical interviews over Zoom and Microsoft Teams. Candidates are evaluated on technical merit, and offers proceed to background screening — with system access provisioned after a successful check.

Challenge

What that process cannot see is the device and network environment a candidate is operating from. A candidate can present a clean resume, pass a technical assessment, and clear a background check while connecting through a multi-hop proxy chain designed to obscure their physical location.

Since at least 2022, the **Democratic People's Republic of Korea** has operated structured programs deploying IT workers globally to generate hard currency for the regime — revenue assessed to support sanctions evasion and weapons programs. These operatives pose as US-based nationals, apply for remote technical positions, and if hired, funnel earnings back to the North Korean government. Individual workers can earn up to $300,000 annually; the North Korean government retains up to 90% of those earnings.

FAMOUS CHOLLIMA doubled its fraudulent employment operations in 2025 vs 2024 and remains the most active threat cluster targeting technology hiring pipelines.

> **We were interviewing candidates who looked legitimate on paper, passed technical screens, and had clean background profiles. The signals imper.ai surfaced — VPN infrastructure, remote access tooling, and network latency mismatch — were not visible in our existing process.**

CISO, Leading Technology Company

Risk & Impact

1 in 4
candidate profiles worldwide will be fake by 2028
Gartner, February 2026

x2
increase in FAMOUS CHOLLIMA fraudulent employment activity in 2025 vs. 2024

122 days
median dwell time for DPRK IT worker incidents before detection
Mandiant M-Trends 2026

$300K
maximum annual salary an individual DPRK IT worker can earn, with up to 90% remitted to the regime
US Department of Justice / Unit 42

Solution

Four candidates exhibiting **high-confidence DPRK IT worker indicators** were identified and removed from the hiring pipeline before any offer was extended. imper.ai's Impersonation Detection Engine ran silently across every interview session — analyzing device, network, and identity signals at each touchpoint and correlating findings across sessions rather than evaluating each in isolation.

Across all four candidates, imper.ai detected Astrill VPN, AnyDesk running during live interviews, and geographic latency irreconcilable with a US location — signals that exist only at the infrastructure layer, invisible to background checks, skills assessments, and ID + Selfie services.

How it works

For hiring fraud, imper.ai's Impersonation Detection Engine carries the full verification weight. Candidates have no work history with the organization — there is no prior context to verify against. The engine analyzes infrastructure-layer signals across multiple hiring touchpoints, not a single point-in-time check.

imper.ai analyzes device, network, and identity signals at every stage — application, screening, technical interview, and offer. Signals are correlated across sessions, not evaluated in isolation. A candidate who presents clean signals at screening but shows Astrill VPN and AnyDesk at the technical interview is flagged on the pattern.

The system integrates directly into Greenhouse and Workday. Detection runs in the background during live sessions on Zoom, Microsoft Teams, and Google Meet. Recruiters do not change their process. imper.ai surfaces a risk signal and correlated case history for review.

Outcome

No access provisioned

All four candidates were removed before offers, credentials, or onboarding steps were initiated.

Interview-layer detection

The identifying signals were invisible to background checks, skills assessments, and standard ID verification.

Downstream systems protected

Source code repositories, cloud infrastructure, and engineering tooling remained secure.

imper.ai

imper.ai is a Workforce Identity Security platform built to detect and stop impersonation attacks across the employee lifecycle. As MFA adoption has increased, threat actors have shifted to the workforce workflows surrounding identity — help desk recovery, MFA re-enrollment, credential issuance, and hiring. imper.ai addresses that gap through real-time infrastructure-layer signal analysis and AI-Driven Contextual Verification, integrated into the platforms security and IT teams already operate.

Get a demo!