imper.ai

SOLUTION BRIEF

Stop insider threats with continuous workforce verification

Hiring verifies who you onboard. Nothing verifies who shows up after.

Once an account is active, no control re-checks who is operating it. Candidates hand roles to offshore proxies. Organized rings resell employment. North Korean (DPRK) IT workers operate through laptop farms. Adversaries inherit accounts to steal IP or pose as an insider threat. Each case looks normal at the activity layer. The drift is at the infrastructure layer.

imper.ai closes this gap with the Impersonation Detection Engine, embedded into existing IDP, MFA, and PAM workflows. Network, endpoint, and behavior signals run seamlessly behind every privileged action and every periodic re-verification you trigger. The user behind the account, not just the credential in front of it.

Where the shadow workforce hides

Detect operator handoff after Day 1
A candidate passes the interview. Someone else does the job. The pattern ranges from benign (job-sharing, offshoring for a cheaper salary) to malicious (IP theft, illicit funding of nation-state programs).

Verify unknown and unverified workforce
Contractors, BPO agents, M&A-inherited accounts, and legacy users often never went through identity proofing. You don't know who they are, only that the account is active.

Security Benefits

Operator-level verification
Detect when the person behind the account changes.

Prevention, not post-detection
Catches infrastructure drift *inside* the step-up workflow, before the privileged action completes.

No documents, no biometrics
Infrastructure-layer signals only. Nothing to forge, nothing to deepfake, no PII exposure.

Operational Benefits

No new prompts, no new tools
Embeds into existing IDP, MFA, and PAM workflows.

Coverage for unknown workforce
Verify contractors and M&A-inherited accounts.

Policy-driven cadence
Trigger re-verification on your schedule. Every two weeks, every month, every six months. You set it.

How imper.ai verifies the user, every time it matters

imper.ai analyzes infrastructure-layer signals (network, endpoint, behavior) and runs them seamlessly inside existing IDP, MFA, and PAM step-up workflows. Drift from the established baseline surfaces immediately.

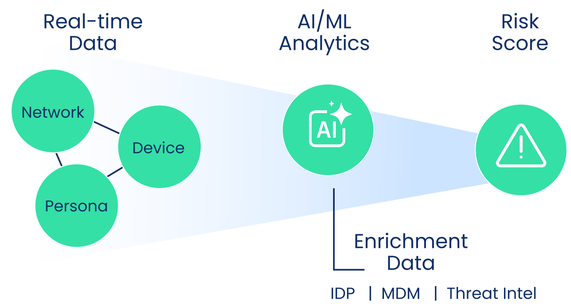
Workforce Trigger

Privileged Action

Step-up Auth

Periodic, Checks

Impersonation Detection Engine



User Verified

Privileged action proceeds, or step-up escalates to security team on drift detection.

1

Infrastructure signal capture

When an employee performs a privileged action or hits a scheduled re-verification, imper.ai seamlessly captures network, endpoint, and behavior telemetry inside the existing IDP, MFA, or PAM step-up.

2

Correlate against the baseline

Signals are correlated against the user's historical data and, where available, the identity-binding moment captured at hire (with imper.ai for Hiring) or at secure enrollment.

3

Generate a risk score

The Impersonation Detection Engine produces a real-time risk score from the correlated signals. The score reflects the likelihood that the user behind the account is impersonating the person you thought you hired.

4

Verify or alert

Low risk: the privileged action proceeds. No friction.
High risk: the action is held and your security team receives an alert for confirmed insider threat or potential impersonation.

User verified — Privileged action proceeds. No friction for the user. No alert noise for the SOC.

Confirmed insider threat or potential impersonation — Action is blocked. Security team receives an alert.

Sample Detection Signals

- Anomalous & Unmatching Location
- Latency mismatches
- Masked Network Connection
- Virtual Machine
- Remote-Controlled Device
- Clean Device / Burner Environment

imper.ai was founded by cyberintelligence experts to stop workforce impersonation and social engineering attacks that route around authentication. Built specifically for workforce identity risk, the platform verifies the operator behind the account, not just the credential in front of it.

imper.ai

Get a demo →