Post-hire verification

The person you hired may not be the person behind the activity.

A new hire can pass every identity and background check, then hand their credentials and company laptop to someone else who does the job remotely. The handoff can happen at any point from day 1 until offboarding, long after hiring and onboarding checks are complete.

How the handoff happens

- **Malicious from the start:** the hire was always a front for someone else, such as an operator working from a sanctioned country.
- **Outsourced work:** a real employee quietly passes the job to someone else, often for a lower wage.
- **Credentials handed over:** the password, MFA and company laptop now serve a person you never vetted.
- **Remote operation:** the new operator works the device through screen-sharing software or remote-control hardware, often from a laptop farm.

Why it matters

- **Full insider access:** whoever is at the keyboard controls everything the employee can reach, from source code to customer data and payment systems.
- **Every control passes:** valid credentials, enrolled MFA and a managed device. Nothing looks wrong to identity and access tooling.
- **Compliance exposure:** customer, financial or medical data can end up in front of someone you never vetted, in a country where it must not be accessed, sanctioned or not.
- **Late discovery:** the handoff can start at any point in the employee's tenure, well after hiring controls have stopped looking.

> **The control gap:** background checks, ID verification and MFA confirm an identity at a point in time. They do not confirm that the *human you hired* is the one at the keyboard on day 90.

What imper.ai detects (examples, not an exhaustive list)

Screen-sharing & remote-access software

Dedicated remote-access tools, and legitimate software used in anomalous ways, such as a day-long Zoom screen-share session.

Remote-control hardware

KVM-over-IP devices that let an operator drive the laptop from somewhere else.

Laptop-farm patterns

Network layouts consistent with a laptop farm hosting company devices on behalf of remote operators.

Location

Hidden or inconsistent locations that don't match the employee you hired.

Anomalous usage

Device and usage patterns that change in ways consistent with a different person doing the work.

Verify continuously, from day 1 onward

Option 1

Lightweight script

Ephemeral: runs the checks without installing anything that stays on the device.

Option 2

Agent

Installed on the device for continuous coverage throughout the employee's tenure.