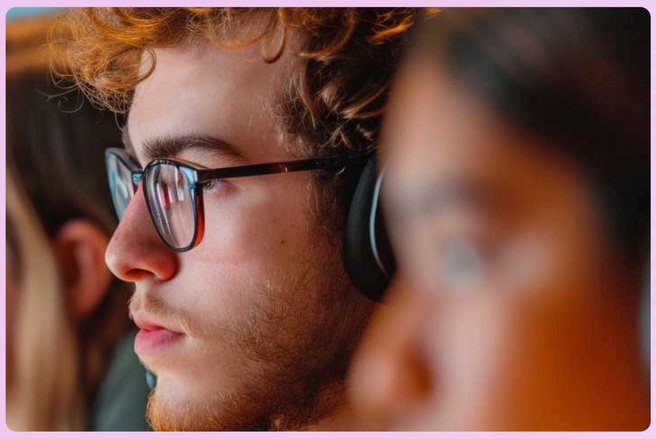
imper.ai

SOLUTIONS BRIEF

Protect your help desk from impersonation attacks

Block social engineering and AI-driven impersonation before it reaches your help desk.



imper.ai exposes impersonation risk behind every request

Impersonation sits at the center of today's workforce and help desk threats. With generative AI, adversaries can now clone voices, create deepfake videos, and convincingly mimic trusted identities, making real-time deception nearly impossible to spot.

imper.ai closes this blind spot by detecting the signals attackers can't fake. Our platform automatically detects risk in every help desk interaction - including those handled over Amazon Connect - in real time through device, network, and behavioral signals correlated with internal HR and identity data. The result: fewer manual checks, faster resolution times, and stronger protection against the most common form of social engineering.

Security Benefits

Prevents impersonation attacks
Stops fake password and MFA reset scams instantly.

Procedure Integrity
Automated flows eliminate bypass attempts.

Strong validation process
Multi-layer verification prevents impersonator authentication.

Operational Benefits

Reduced Workload & Costs
Minimizes manual verification steps and free up IT resources.

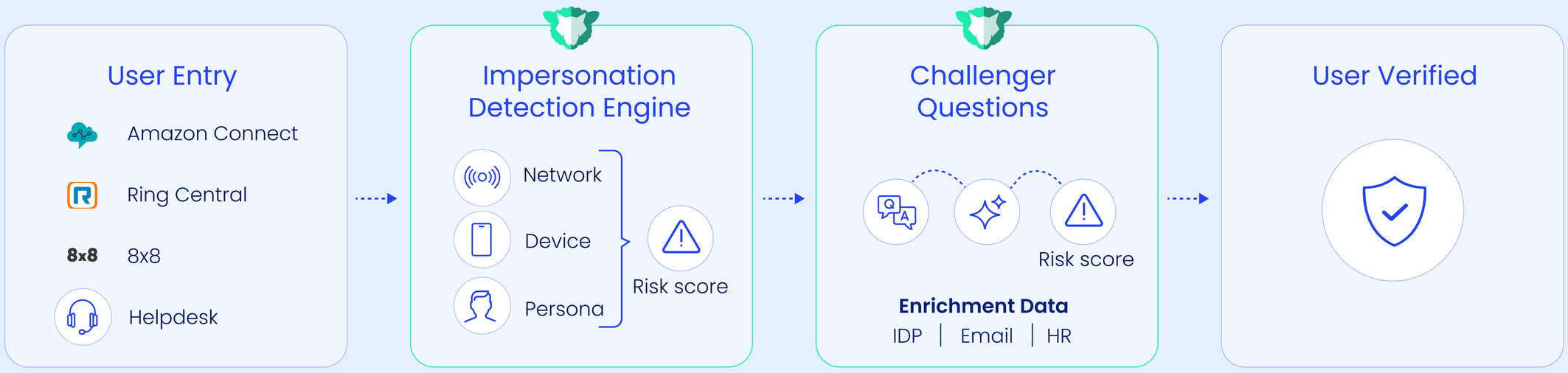
Scalable, consistent process
Applies uniform checks across teams and regions.

Frictionless experience
Decrease time to resolution with automated workflows.

How it protects your help desk - and your workforce

The imper.ai platform analyzes device, network, and persona signals, correlating them with identity, HR, and communication data to verify each requester. imper.ai assesses environmental and behavioral signals in real time to detect signs of manipulation or impersonation, for large workforces, help desk agents can't rely on recognizing every caller or employee, making traditional resets easy to exploit. imper.ai strengthens these recovery flows by validating users through objective, data-driven signals rather than familiarity or guesswork.

Next, the requester is presented with dynamic questions drawn from internal data. These layers combine into a single risk score that determines whether to approve, escalate, or block the request — seamlessly integrated within Amazon Connect and your existing ITSM stack.



1

Employee Request

The requester contacts the IT help desk via Amazon Connect or the IVR provider and requests a password reset. The agent or the IVR issues an imper.ai verification link.

2

Impersonation Detection

imper.ai scans the security signals of the requester for signs of suspicious activity before automatically moving onto the Challenger Questions.

3

Knowledge Check

The requester will be presented with a number of questions related to internal knowledge. They answer via free text which is then analyzed by imper.ai's LLM to produce the final score.

4

Automated Outcomes

Once verified, the agent can send the requester the password reset link or drop the ticket if the requester is malicious. If integrated with your ITSM this can all be done automatically.

imper.ai was founded by cyberintelligence experts to stop workforce impersonation and AI-driven social engineering attempts that bypass authentication controls. Built specifically for workforce identity risk, the platform verifies both the environment and the operator before trust is granted.

imper.ai

© imper.ai 2026 . All rights reserved. Proprietary and confidential. Subject to change without notice.

Book a demo today →