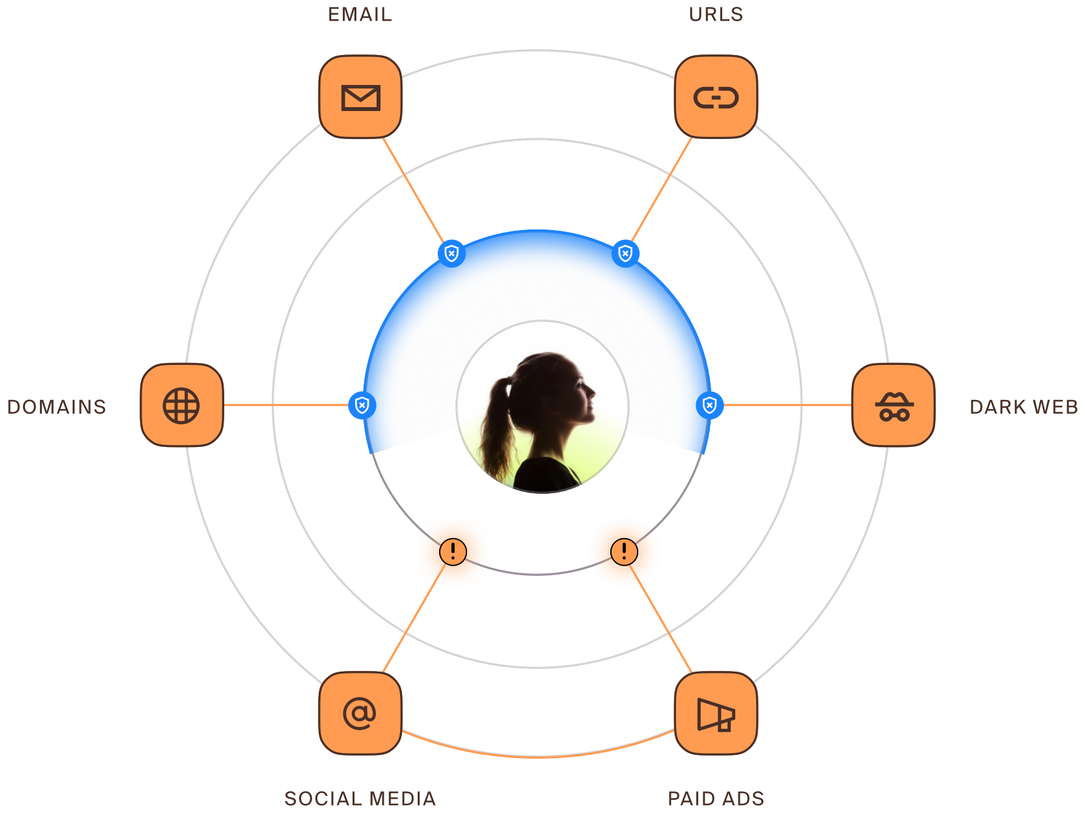
MULTICHANNEL VISIBILITY

Doppel

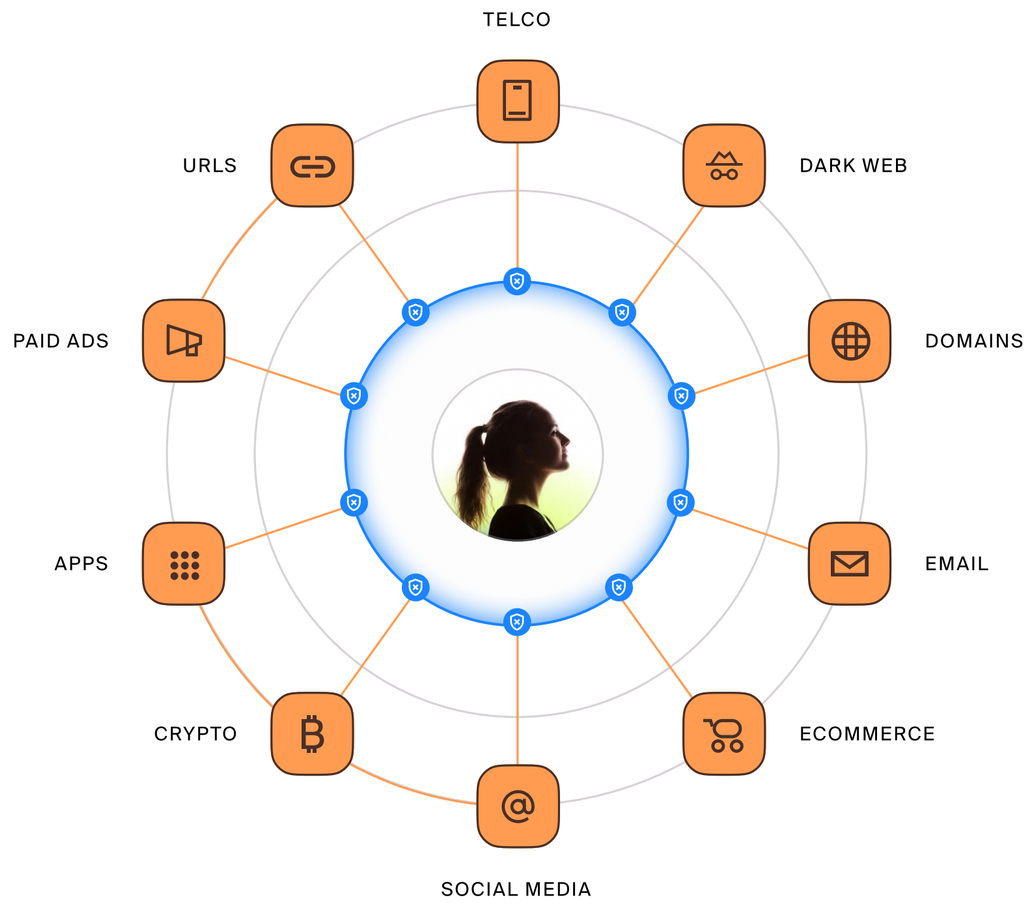
Detect and Disrupt at the Point of Attack

A Case of Linking Multi-Channel Defense

Legacy vendors can’t defend against multiple emerging channels



Multi-channel attacks need multi-channel protection



The Problem: AI Has Outpaced Your Defenses

Social engineering is now the dominant cyber threat vector, supercharged by AI. Attackers exploit blind spots across: Social platforms (LinkedIn, TikTok, X), Messaging apps (Telegram, WhatsApp), Paid ads, SMS, rogue apps, and spoofed domains, Dark web markets and crypto platforms. Yet most security teams only monitor 2–3 of these surfaces, often in silos.

The result? Fragmented visibility, slow takedowns, and missed threats.

Why It’s Getting Worse

AI lowers the barrier of entry for mass-scale impersonation and phishing. Attacks now span multiple surfaces in coordinated campaigns. Legacy tools can’t detect cross-channel campaigns or automate threat disruption and takedown.

Doppel

Real-World Consequences

$243K

lost in a deepfake voice scam targeting finance execs.

SOURCE: WSJ

6%

stock drop at Eli Lilly due to Twitter impersonation.

SOURCE: FIERCEPHARMA, 2022

MILLIONS

lost to fake support agents on Telegram and Reddit.

SOURCE: FBI, 2023

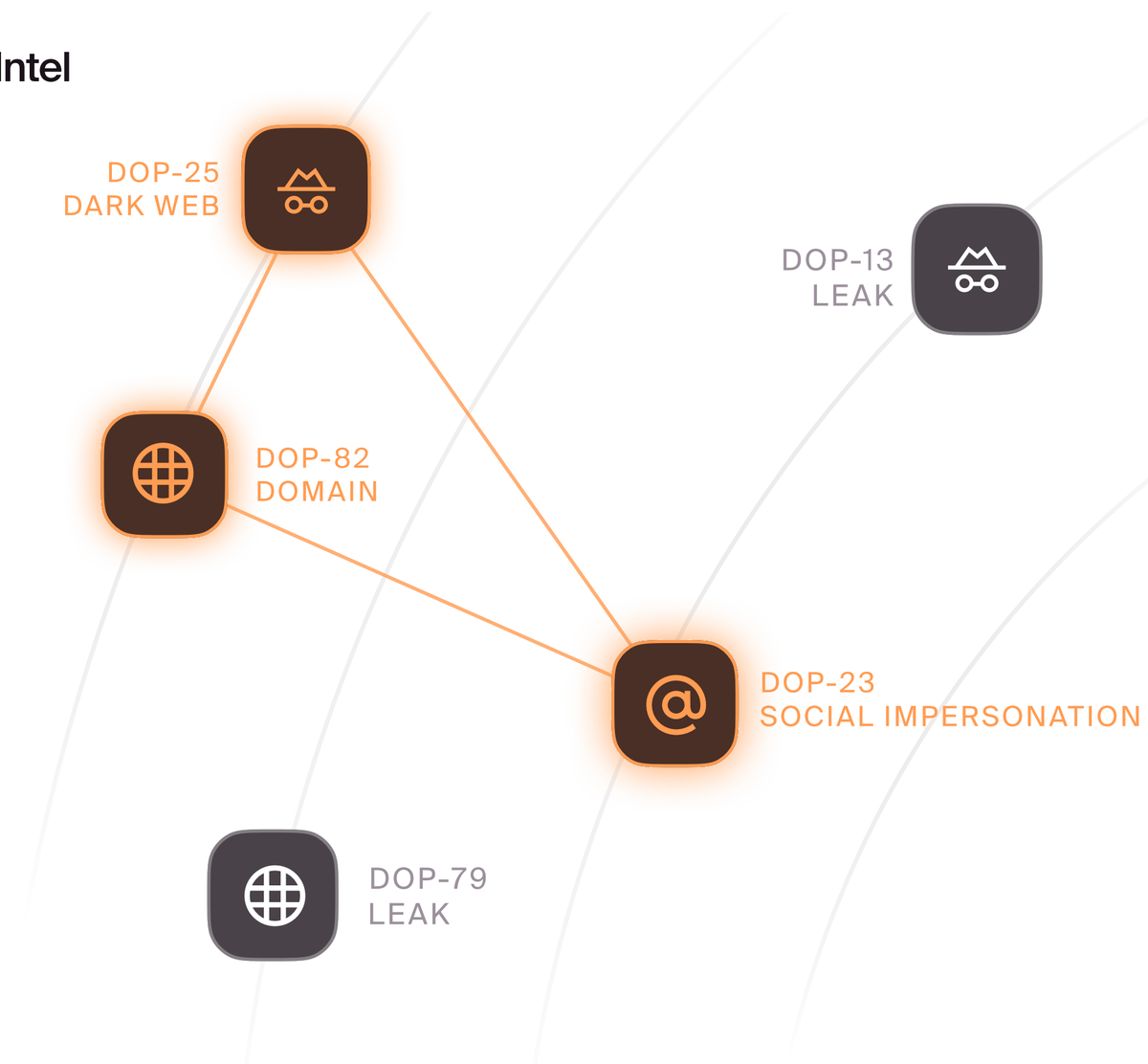
The Solution: Linked, Multi-Channel Defense

To defend against deception at scale, teams need a modern, multi-channel defense platform with:

- Continuous scanning across all digital surfaces
- Graph-driven detection of linked infrastructure and signals
- Automated takedowns via APIs and registrar integrations
- Cross-team workflows to unify Brand, SOC, Fraud, and Threat Intel

Next Steps for Security Leaders

- Audit visibility gaps across all surfaces
- Unify teams & workflows
- Deploy graph-powered detection
- Automate takedowns
- Simulate modern threats like AI phishing and voice clones



Book your demo at doppel.com/request-a-demo