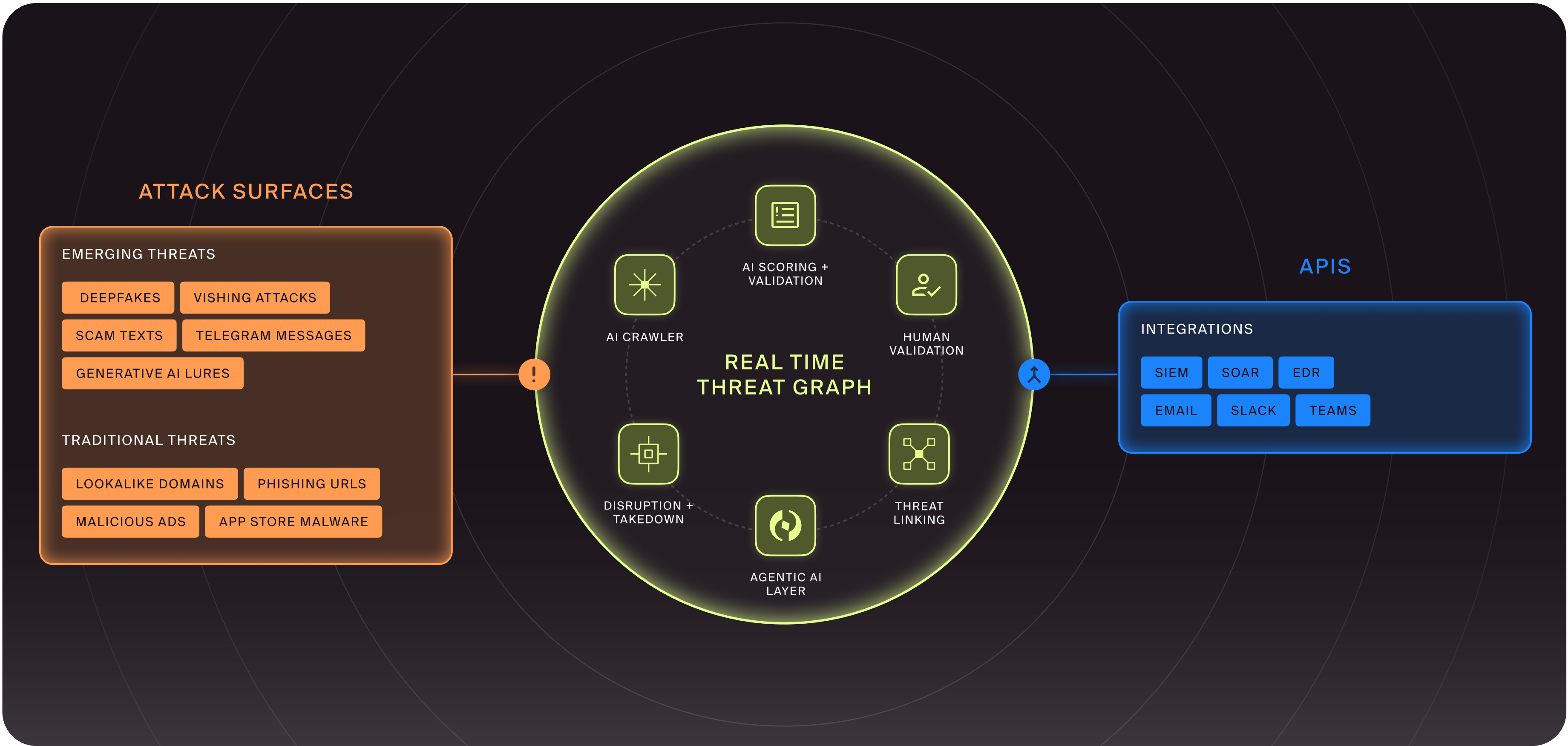


Introducing the Doppel SED Platform

The AI-native platform designed for Social Engineering Defense.

How Doppel SED Works

Doppel protects individuals and brands from AI-powered impersonation, phishing, fraud, and social engineering by dismantling attacker infrastructure and building resilience through targeted training and simulation.



✔ Multi-Channel Monitoring & Detection

Continuously scans across 100+ languages and surfaces, including Telegram, WhatsApp, and the dark web.

✔ Agentic AI & Multi-Step Simulations

Deploys hyper-realistic, multi-channel simulations (Email, SMS, Voice, Teams) that use conversational threading to mimic real attacker persistence and validate readiness.

✔ Dynamic Behavioral Risk Modeling

Moves beyond vanity metrics to quantify risk by department and role, using live threat data to drive targeted training and "just-in-time" coaching.

✔ Automated Infrastructure Disruption

Enacts cross-platform enforcement in minutes by dismantling the operational core of fraud—targeting "sticky" indicators like phone numbers and ad IDs to kill attacker ROI.

Products powered by the Doppel SED Platform



Brand Protection

Detect, correlate, and dismantle impersonation threats targeting your brand across all digital channels.



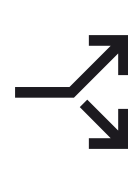
Executive Protection

Safeguard high-profile leaders by detecting and disrupting synthetic media, deepfakes, and personal data exposure.



Simulation

Test people and processes against realistic, agentic AI-powered simulations to reduce risk exposure.



Security Awareness Training

Strengthen defenses with role-specific, deepfake-driven training content and personalized coaching.

Trusted by



The SED Architecture

The Doppel SED architecture converges Digital Risk Protection (DRP) and Human Risk Management (HRM) into a single, agentic system. It moves security from reactive event-handling to a continuous disruption loop.



How Doppel SED Works

Doppel protects individuals and brands from AI-powered impersonation, phishing, fraud, and social engineering by dismantling attacker infrastructure and building resilience through targeted training and simulation.

✓ Multi-Vector Ingestion

Doppel continuously ingests signals from the entire external attack surface (domains, social, ads, telco, and the dark web) alongside internal signals from employee phishing reports and simulation results.

✓ The Real-Time Threat Graph

The central nervous system of the platform. It links disparate artifacts (IPs, ad IDs, phone numbers) into a unified Campaign View, revealing the full scope of an attacker's infrastructure. This informs training and simulation campaign recommendations based on real-world insight.

✓ Closed-Loop Resilience

Every external threat detected is fodder for threat-informed simulation campaigns. Every external threat detected informs simulation campaigns with real-world attacker tactics.

✓ Agentic AI Reasoning

Using LLMs trained on expert security data, Doppel's agents autonomously triage threats, prioritize high-risk campaigns, and map out the necessary takedown steps.

Core Infrastructure Components

Networked Intelligence Engine

Connects cross-campaign attacker patterns so that every takedown for one customer enriches the defense for all.

Cross-Vector Enforcement

Orchestrates automated API-driven takedowns across registrars, hosting providers, social platforms, and telco carriers simultaneously.

Adaptive Behavioral Model

Correlates real-world attack data with internal employee performance to produce a dynamic Heatmap of Risk across the organization.

Zero-Day Detection by Design

Doppel's agents evaluate based on attack behavior and infrastructure relationships, not a known-threat list. Even when an attack has never been seen before using brand new techniques, Doppel still detects the threat.