HUMAN RISK MANAGEMENT OVERVIEW

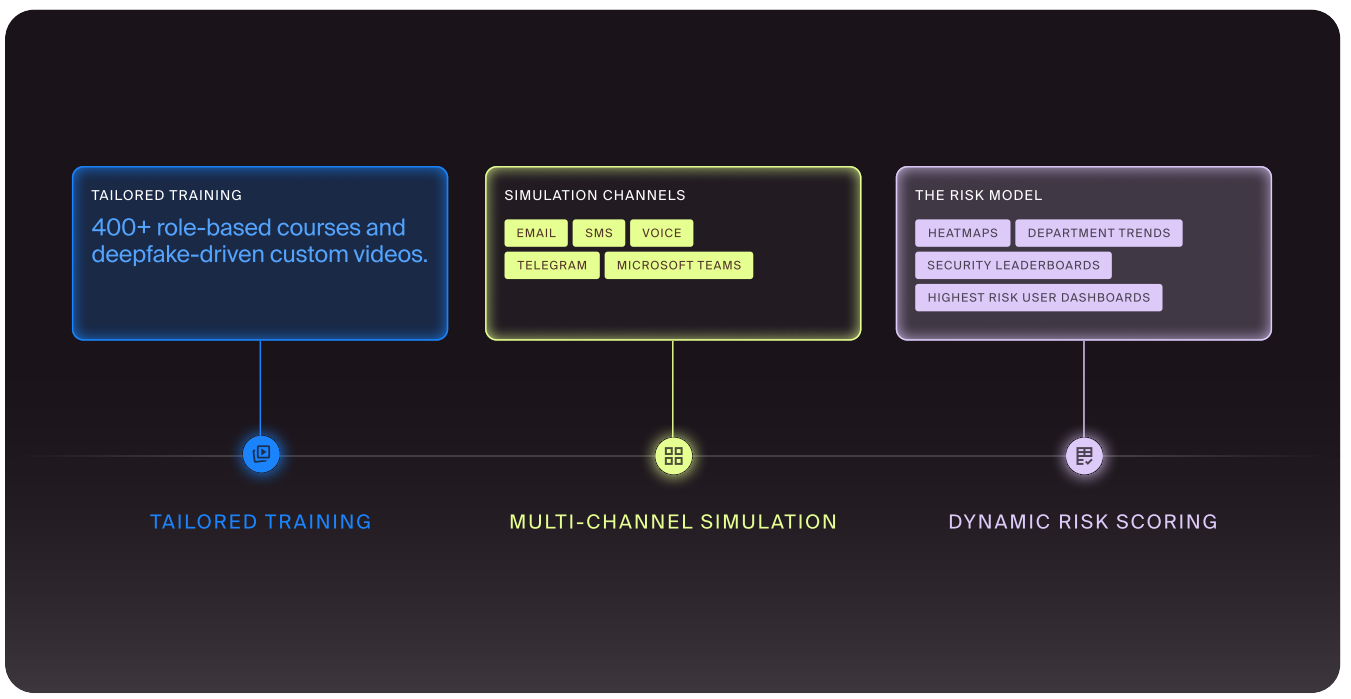
Doppel

Introducing Doppel Human Risk Management (HRM)

Turning education into measurable resilience against modern attacks.

How Doppel HRM Works

Social engineering is the primary entry point for 98% of attacks, and median users click a phishing link in under 60 seconds. Doppel HRM goes beyond click rates to focus on changing human behavior and quantifying risk.



Agentic AI-Powered Simulations

Hyper-realistic simulations that traverse channels, using conversational threading to mimic real attacker persistence.

Deepfake-Driven Training

Generates role-specific video training featuring deepfakes of executives or employees, delivering lessons based on real-world intelligence or company policies.

Dynamic Risk Modeling

Move beyond vanity metrics to identify high-risk teams—including Helpdesks or BPOs—for targeted remediation.

Closed-Loop Resilience

A threat detected on the open web today becomes a "Just-in-Time" training module tomorrow.

Strategic HRM Use Cases

Breach Prevention

Expose and eliminate susceptibility in privileged user groups before access can be exploited.

Helpdesk and BPO Security

Strengthen defenses at the frontline by simulating voice-cloned "urgent" executive requests.

Adversary Emulation

Red teams pressure-test resilience with multi-step attacks based on live TTPs or insider risk scenarios.

Audit-Ready Compliance

Provides demonstrable evidence of security controls, training, and simulation exercises for SOC 2, ISO 27001, PCI, and more.

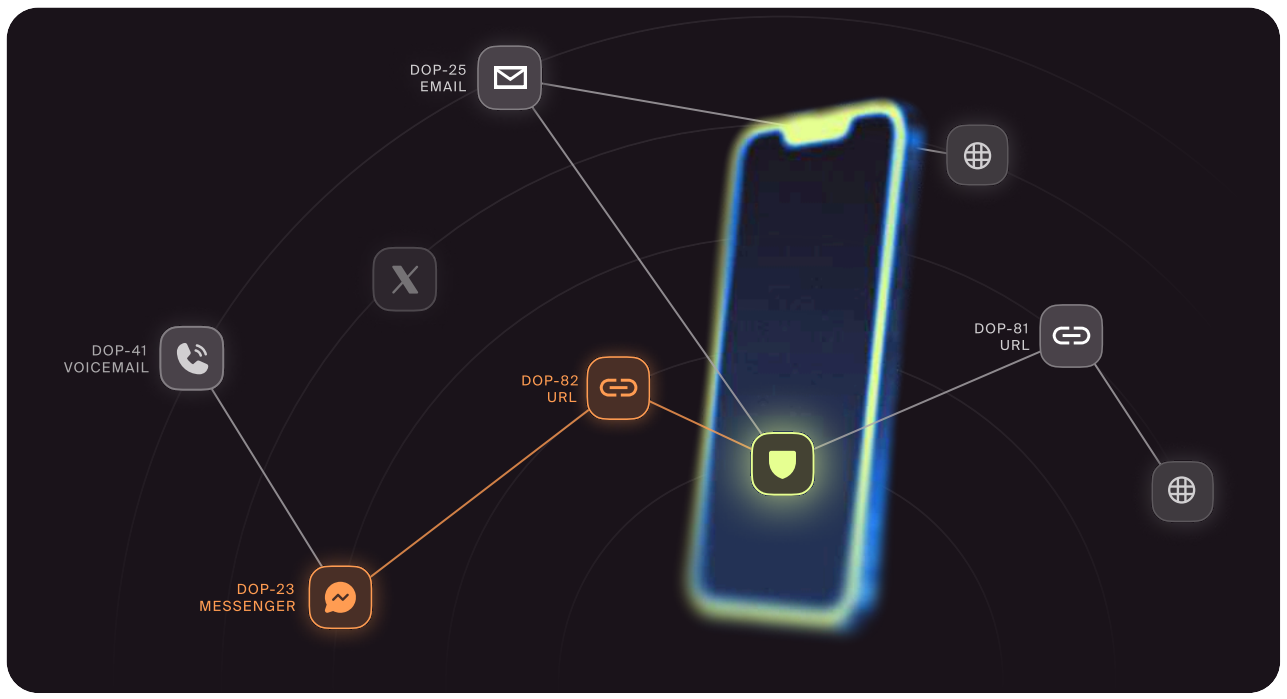
Trusted by OpenAI Tripadvisor ramp shopify

HUMAN RISK MANAGEMENT OVERVIEW

Doppel

The HRM Architecture

The Doppel HRM architecture is designed to turn the human element from a vulnerability into a sensor network by synchronizing real-world intelligence with behavioral science.



The HRM Resilience Engine

Using the HRM resilience engine, you get clear insights into where risk lives and how it evolves, informing technical control and policies.

AI Phishing Agents

Unlike static templates, Doppel's architecture uses AI agents capable of multi-step conversational threading. These agents can move from an initial email to a voice call or an SMS, mimicking the persistent, cross-channel tactics of modern adversaries.

Phishing Triage

A critical architectural component that empowers employees to report suspicious emails directly from Outlook or Gmail. These reports are triaged in seconds by LLMs trained on Doppel's global threat intelligence, providing instant feedback to the user.

Generative Content Factory

The architecture includes a native generative AI engine that creates deepfake-driven training content. By uploading a short clip or image of an executive, security teams can generate custom, high-impact training videos tailored to specific milestones or real-world threats.

Architecture for Data-Driven Risk Modeling

Role-Based Susceptibility Scoring

The platform calculates risk not just on clicks, but on the potential impact of the user. An engineer with access to the production codebase is weighted differently than a marketing intern, allowing CISOs to prioritize controls.

BPO and Helpdesk Extension

Specialized architecture for testing outsourced frontline defenses. Doppel's vishing agents can autonomously navigate IVR phone trees and hold times to test if helpdesk agents follow security protocols when faced with an "urgent" request.