DIGITAL RISK PROTECTION OVERVIEW

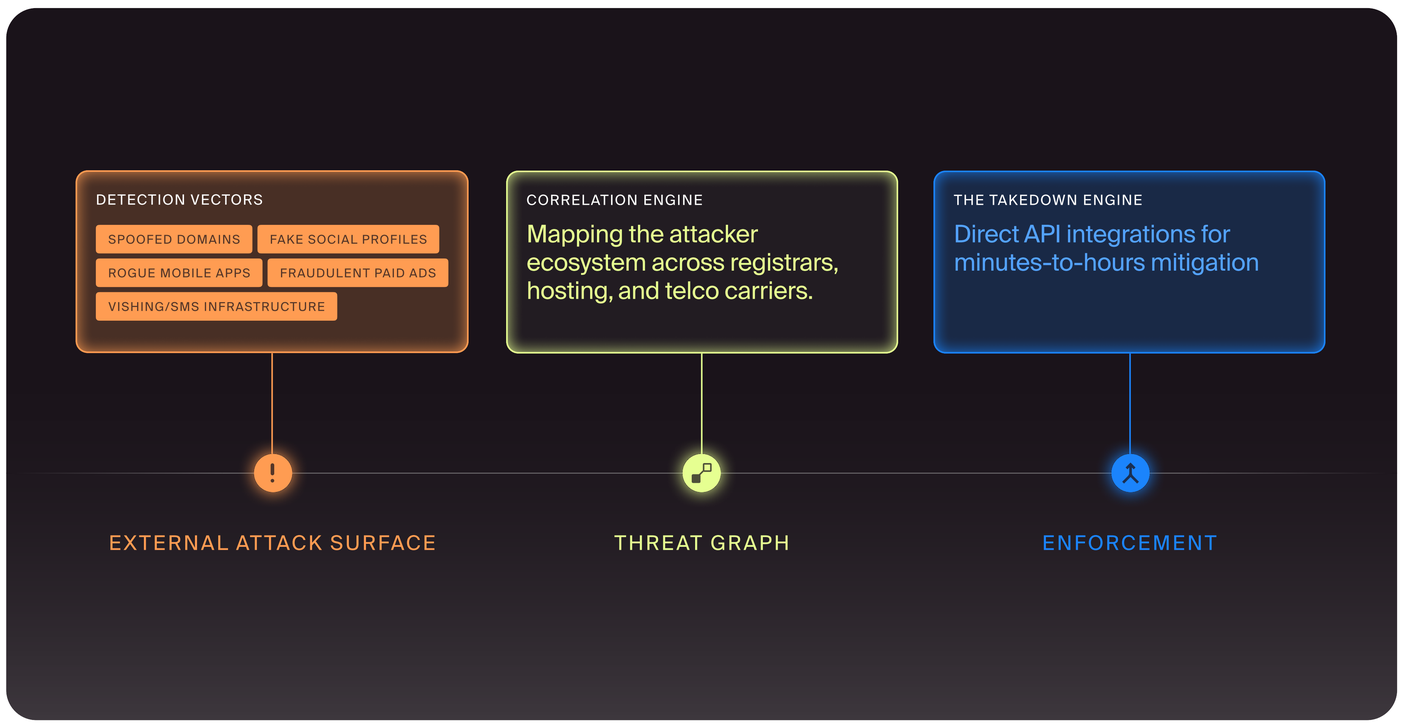
Doppel

# Introducing Doppel Digital Risk Protection (DRP)

Active offense designed to outpace machine-speed attacks.

## How Doppel DRP Works

With a 1,000% increase in phishing volume, legacy alert-and-triage models are obsolete. Doppel DRP provides a campaign-level view of external fraud, identifying and dismantling threats before they evolve into internal breaches.




### Continuous Attack Surface Mapping

Real-time visibility into diverse threat vectors, even where traditional tools have blind spots.

### AI-Native Infrastructure Disruption

Moves beyond "whack-a-mole" by targeting sticky indicators like phone numbers and ad IDs.

### Graph-Driven Campaign Mapping

Connect the dots from a fake account to a spoofed site to a dark web listing to see the full campaign.

### Automated Incident Response

Turn inbound reports into actionable threat intel, reducing manual SOC workload.

## Measurable DRP Outcomes

### Time-to-Disruption

Reduce takedown time from days to minutes, with a median mitigation for phishing domains in under 1 hour.

### Attacker ROI Reduction

Targets the operational core of fraud campaigns to cut the risk surface down to zero.

### Executive Safety

Neutralize synthetic media targeting the C-suite with fringe platform detection.

### SOC Efficiency

Automate triage and enrichment, transforming user reports into a high-impact sensor network.

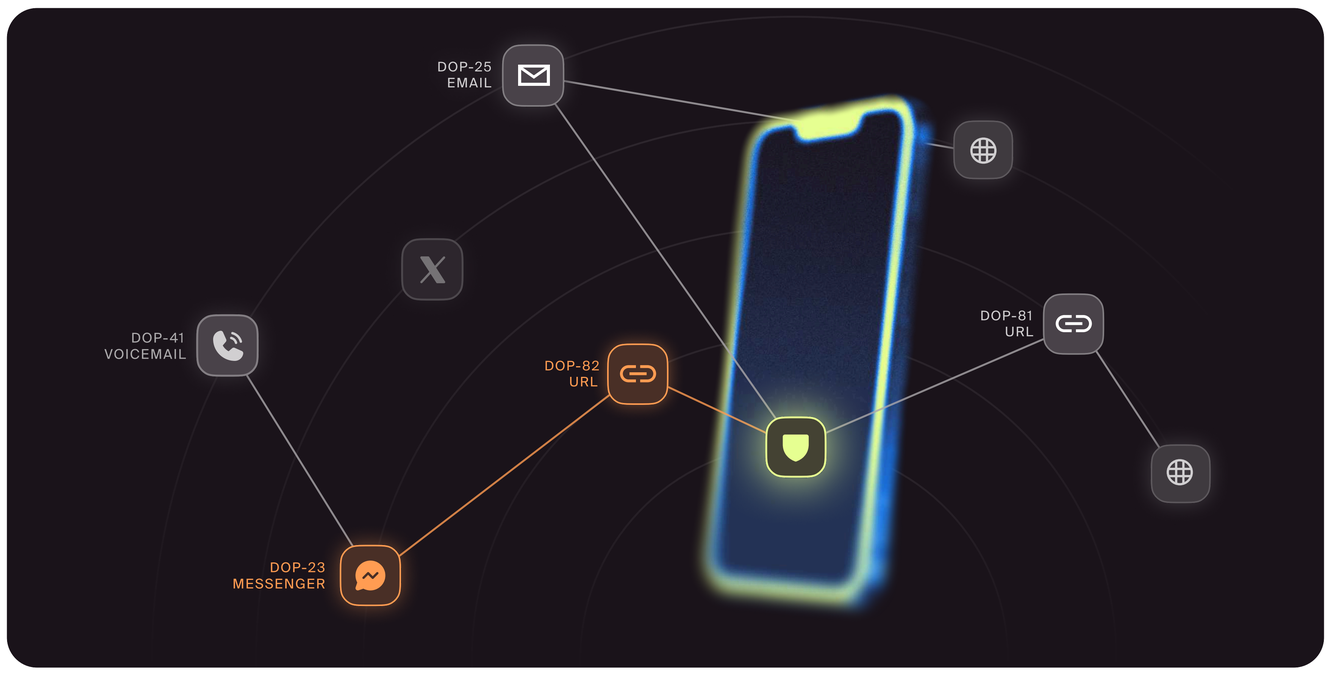
Trusted by OpenAI Tripadvisor ramp shopify

DIGITAL RISK PROTECTION OVERVIEW

Doppel

# The DRP Architecture

The Doppel DRP architecture is built for machine-speed elimination, moving beyond simple detection to dismantle the infrastructure that enables deception.




## Architectural Pillars of Disruption

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.

### The Global Ingestion Layer

Doppel monitors over 1 billion indicators daily across 100+ languages. This includes non-traditional surfaces like Telegram, WhatsApp, and specialized dark web markets where attackers stage campaigns.

### The Threat Graph

Instead of generating isolated alerts for every domain, the architecture uses graph-based logic to link artifacts back to a single root cause infrastructure. It maps sticky indicators (phone numbers, ad IDs, and hosting patterns) that are expensive for attackers to replace.

### Agentic Takedown Workflows

The enforcement layer uses AI agents to automate the legal and technical work of takedowns. By integrating directly with the APIs of registrars, social platforms, and telcos, Doppel achieves a median takedown time of <11 hours for social and ad threats.

## Core Infrastructure Components

### Brand AbuseBox

Architecture that transforms your existing abuse or phishing mailboxes into an automated sensor network. It automatically extracts indicators of compromise and triggers disruption workflows.

### Bidirectional SIEM/SOAR Sync

DRP findings are pushed via webhooks into your existing SOC toolchain (Splunk, Elastic, Tines), ensuring that external intelligence is instantly operationalized for internal defense.