TAKEDOWNS AND ENFORCEMENT

Doppel

Autonomous disruption for modern social engineering

Threat campaigns move across platforms at machine speed. Doppel's agentic Social Engineering Defense platform maps adversary infrastructure, correlates threats across channels, and dismantles entire campaigns at scale.

Human trust is now the primary attack surface.

Attackers no longer rely on isolated phishing emails or single fake accounts. Today's campaigns span domains, social media, messaging apps, paid ads, fake support channels, AI-generated impersonations, and deepfakes simultaneously, evolving faster than security teams can respond.

Most Digital Risk Protection (DRP) providers operate passively: monitoring threats, generating alerts, and playing whack-a-mole with individual takedowns. But alerts don't stop attacks. Removing one domain, profile, or ad doesn't stop the campaign behind it.

Doppel was built for the AI era. Our Threat Graph continuously maps attacker infrastructure across channels, linking domains, social accounts, ads, messaging, apps, and supporting infrastructure into coordinated campaigns.

Doppel then executes rapid, high-confidence takedowns that disrupt the attack at its source, reducing customer harm, reputational risk, and operational burden before threats spread.

Median Takedown Times

< 10 HOURS
OVERALL

< 7 HOURS
SOCIAL MEDIA

< 5 HOURS
PAID ADS

< 12 MINUTES
MALICIOUS SITES BLOCKED

The Doppel Difference

100%
IN-HOUSE TAKEDOWNS

95%
OF CLOUD-HOSTED THREATS MITIGATED

Common Use Cases

Multi-channel phishing campaigns:
Domains, fake login flows, messaging abuse, social impersonation, and paid ads working together to steal credentials and distribute malware.

AI-enabled impersonation:
Deepfakes, cloned executive identities, fake support agents, and synthetic personas used to deceive employees and customers.

Brand & executive impersonation:
Fraudulent social accounts, spoofed domains, fake apps, and impersonation campaigns targeting trust and reputation.

Consumer fraud & account takeover:
Fake customer support, refund scams, loyalty fraud, credential theft, and account abuse across digital channels.

Employee-targeted social engineering:
Recruiting scams, payroll fraud, vendor impersonation, MFA bypass attempts, and help desk deception.

Persistent attacker infrastructure:
Coordinated campaigns spanning domains, messaging, hosting, ads, telco infrastructure, and social ecosystems.

Unparalleled Social Coverage

Alibaba apps
BlueSky
Discord*
Facebook*
Instagram*
Kakao
Line
LinkedIn*
Linktree
Medium
Pinterest
Quora
Reddit
Telegram*
Threads
TikTok*
Truth Social
Tumblr*
Twitch
Twitter/X
Weibo
WeChat
WhatsApp*
YouTube

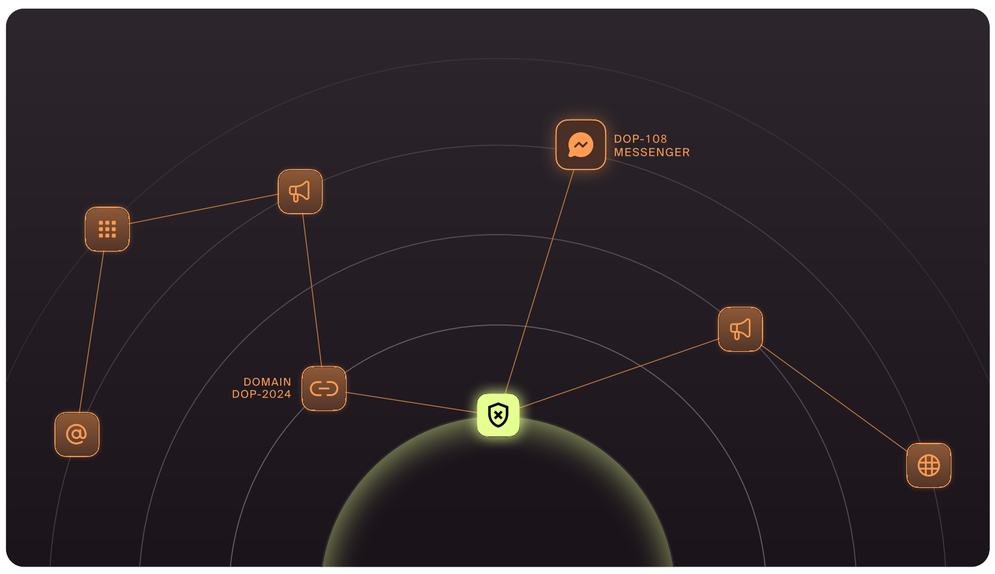
And many more

* Bolded platforms represent channels where Doppel has differentiated disruption capabilities through established platform relationships, escalation paths, and/or proven expertise disrupting malicious content on traditionally difficult-to-remediate platforms.

TAKEDOWNS AND ENFORCEMENT

Doppel

Detection alone doesn't stop threat campaigns. Doppel does.



Most DRP solutions focus on identifying individual threats: a phishing domain, a fake profile, a scam ad, a spoofed account. But attackers operate coordinated campaigns across channels, infrastructure, and platforms simultaneously.

By the time one artifact is removed, the campaign has already shifted elsewhere. Doppel combines Threat Graph correlation, AI-driven enforcement workflows, and 24/7 takedown operations to dismantle the infrastructure behind coordinated attacks, reducing customer harm before threats can scale.

How it Works

Threat Graph correlation

Doppel continuously maps relationships between attacker infrastructure, identities, behaviors, domains, social accounts, ads, messaging activity, and supporting services to expose the full campaign.

Agentic enforcement workflows

AI-driven workflows investigate, enrich, prioritize, and prepare high-confidence takedown actions across platforms and providers. In edge cases where provider constraints limit automation, hybrid workflows ensure reliable execution and uninterrupted coverage.

Infrastructure-first disruption

Doppel targets the infrastructure powering campaigns, registrars, hosting providers, CDNs, ad networks, messaging providers, app stores, and social platforms, not just the visible artifact.

Trusted escalation paths

Direct provider relationships, platform-specific playbooks, and escalation channels accelerate enforcement and improve takedown success rates.

24/7 takedown operations

Dedicated in-house operators manage enforcement globally around the clock, ensuring rapid response as campaigns evolve.

AI-packaged evidence & attribution

Doppel packages enforcement-ready evidence, campaign context, and AI-generated rationale to accelerate reviewer action and improve takedown velocity.

The Outcome

Reduce customer harm

Stop scams, impersonation, and phishing campaigns before they spread broadly across customers and employees.

Protect brand trust

Prevent fraudulent accounts, fake support channels, and impersonation campaigns from damaging reputation and credibility.

Reduce operational burden

Replace fragmented monitoring and manual triage workflows with automated campaign correlation and disruption.

Shrink attacker ROI

Dismantling infrastructure forces attackers to continuously rebuild campaigns, increasing cost and reducing effectiveness.

Stay ahead of AI-enabled attacks

Defend against rapidly scaling AI-driven impersonation and social engineering campaigns built for speed and volume.

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