Doppel

Detect and Disrupt at the Point of Attack

A Case for Linking Multi-Channel Defense

A strategic framework for modern threat disruption.

The Multi-Channel Disconnect

In 2025, social engineering isn't just one of many threats—it's the dominant threat vector in cybersecurity.

AI has given attackers the ability to craft realistic, coordinated, and scalable campaigns that span every corner of the digital landscape: spoofed domains, fake executive profiles, deepfake phone calls, rogue mobile apps, fraudulent ads, encrypted messaging, and dark web chatter.

Yet, most organizations only monitor 2-3 of these surfaces. Even those with advanced tooling are often hampered by siloed teams, fragmented telemetry, and slow manual workflows. The result is a massive Visibility Gap — where threats go undetected not because they're sophisticated, but because defenders simply aren't looking in the right place, or aren't sharing what they find.

And perhaps more dangerously: many aren't looking because they don't believe they need to. Most teams monitor the platforms where they operate or where they've seen threats before. But attackers are more creative than that. If you're not on Telegram, doesn't mean a scammer isn't impersonating you there. If your brand has no crypto product, it doesn't stop someone from launching a fake token in your name. If you're not buying ads on Google, it doesn't prevent someone else from targeting your customers with fraudulent ones.

The most dangerous risks are the ones outside your line of sight.

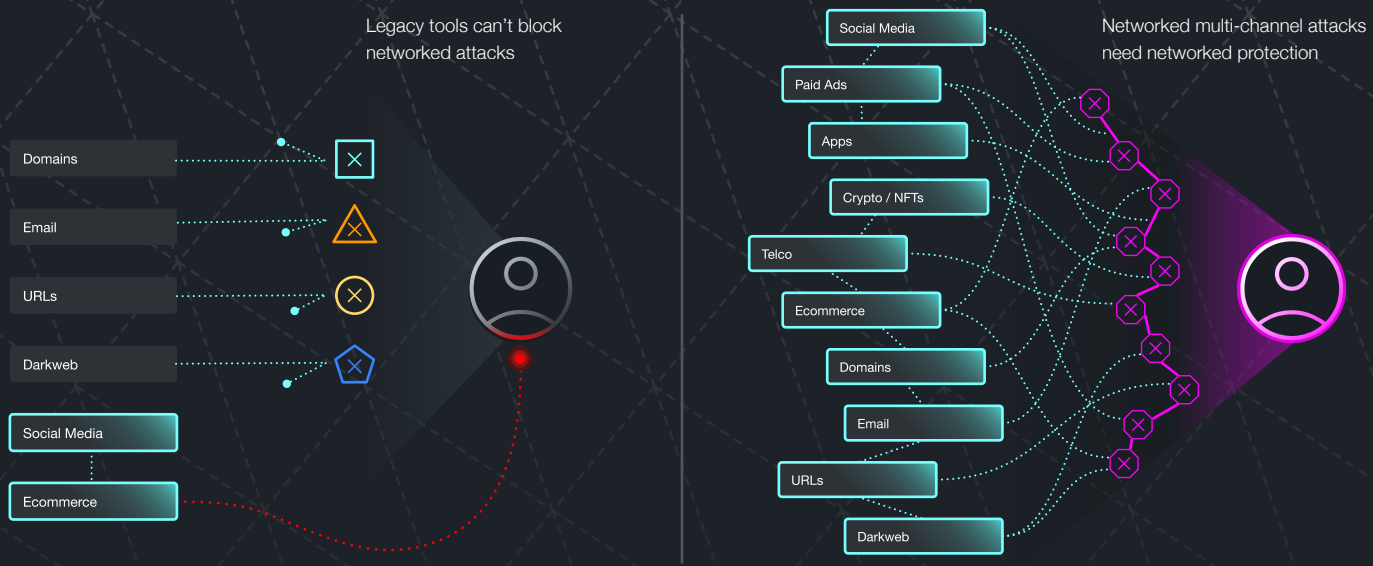
Today, your digital risk surface includes not only the channels you use, but the ones attackers know your customers trust. When you don't show up in those spaces, they will. And without unified visibility, you won't even know until the damage is done.

This guide explores how generative AI supercharged social engineering, why legacy defenses fail to keep up, and how security teams can close the gap with unified, real-time visibility across the modern digital attack surface.

Doppel

Why Most Organizations Can't See What's Targeting Them

Today's attack surface extends far beyond corporate firewalls or inbox. Brands and employees are exposed.



Yet most security stacks are still optimized for internal telemetry and email-based threats.

This leaves critical surfaces like mobile messaging, voice, dark web, and paid media completely unmonitored. According to a 2025 Enterprise Threat Survey:

64% of orgs experienced social engineering attacks via non-email channels

0% were simulating or training for those vectors

Even more striking: many of these attacks happen on platforms brands don't even use. But attackers count on that. They're betting you'll never look where you think you don't belong.

Over 30% of social media impersonation threats in 2023 occurred on fringe or non-primary platforms; places where the targeted brand did not maintain an active presence. Similarly, the Anti-Phishing Working Group (APWG) has reported a growing volume of phishing activity shifting to encrypted messaging apps and rogue app marketplaces, far outside the visibility of most corporate security teams. That's not just a tooling problem. It's a visibility collapse.

Doppel

How AI Unlocked Scalable, Multi-Channel Deception

Generative AI has fundamentally altered the economics of cybercrime.

What once took hours of manual effort is now fully automatable. Adversaries can launch sophisticated, cross-channel deception campaigns at machine speed.

1,760%
Compromised business email attacks up from 2023, largely driven by use of generative AI tools

Source

~140%
Increase of gen AI-based threats in browser-phishing and ~130% jump in zero-hour phishing vs. 2023

Source

$40B
Projected US fraud losses from generative AI by 2027, rising from ~$12.3B in 2023

Source

This is no longer about spotting an isolated phish. It's about defending against AI-powered influence operations designed to exploit trust, across every channel people use to communicate.

The Limits of Legacy Defenses

Legacy security tools weren't built to handle:

Synthetic identities, deepfakes & spoofed AI personas

Real-time, cross-channel correlation

Infrastructure takedown at attacker scale

Instead, most DRP, brand protection, and threat intel solutions flag individual artifacts– a spoofed domain here, a fake LinkedIn profile there– but fail to connect the dots into a unified campaign or disrupt the attacker's infrastructure.

Doppel

Cross-Team Blind Spots Compound the Problem

Brand, SOC, and Threat Intel teams may all detect pieces of an attack. But if no one connects the dots, the campaign succeeds.

Brand notices a fake executive profile spreading on LinkedIn

SOC quarantines a spoofed email from the same attacker

Threat intel surfaces a new phishing kit targeting your sector

But no one sees the whole picture.

Traditional org structures reinforce silos between Brand, SOC, Fraud, and Threat Intelligence teams. Each group works in its own system, on its own timelines, with its own tools.
That means:

- Critical signals get buried or missed
- Context is fragmented
- Response is slow and reactive

Meanwhile, attackers are unified. They launch multi-surface campaigns in real time spanning social, domains, dark web, email, and fringe platforms all coordinated from a single playbook.

Key Limitations of Legacy Tools + Structures

Siloed coverage

Email-only. Social-only. Domains-only. No shared threat graph.

Manual takedown workflows

Slow escalation chains with no real-time disruption.

Alert fatigue

Hundreds of low-context alerts, no campaign-level priority.

No fringe or encrypted channel coverage

Telegram, WhatsApp, paid ads, app stores.

No infrastructure correlation

Artifacts are treated as unrelated, even when part of the same campaign.

Blind to AI-generated deception

These threats slip through outdated filters and static detection rules.

By the time legacy tools stitch the attack together,
the attacker has already executed.

Doppel

Real-World Losses from Fragmented Visibility

The cost of incomplete visibility isn't theoretical. It's measurable.

243k lost in one deepfake voice scam when a CEO's clone called a finance executive

Source: WSJ

6% drop in Eli Lilly's stock after a fake verified Twitter account posted false information

Source: FiercePharma, 2022

> Crypto users exploited via Telegram and Reddit by fake support agents impersonating official reps. Funds stolen, reputations damaged.

> Verified accounts hijacked in Web3 to promote phishing domains. Victims trusted the source and lost assets.

Attackers don't need to breach your perimeter, they just need to **exploit one unmonitored channel.**

The Visibility Revolution: What Modern Defense Requires

Unified visibility is no longer a nice-to-have. It's the foundation for modern social engineering defense.

A Modern Platform Must Include:

Continuous scanning across all surfaces

Social, messaging, web, ads, dark web, apps

Graph-driven detection

Connect domains, bots, profiles, and signals into unified campaigns

Agentic AI correlation

Identify shared infrastructure and automate prioritization

Automated takedown workflows

Remove threats in real-time via API and registrar-level integration

Cross-team integration

Embed into SOC, Brand, and Fraud workflows with shared visibility and escalation paths

Fringe & emerging surface coverage

Protect across overlooked vectors where modern scams begin and legacy tools fail to see.

Doppel

Building Resilience: A Roadmap to Unified Defenses

Security leaders can take action by:

Auditing current visibility
Where are the blind spots? Who owns which surfaces?

Breaking down internal silos
Unify Brand, SOC, Fraud, and Threat Intel workflows into a shared platform

Implementing graph-powered detection
Link seemingly unrelated signals into campaign-level visibility

Automating response at attacker speed
Reduce takedown time from days to minutes with real-time disruption

Simulating modern threats
Test against AI-generated phishing, voice clones, and deepfake scams

You Can't Defend What You Can't See

AI didn't just enhance social engineering, it industrialized it. Modern attackers operate across more channels, with more automation, and more believability than ever before. Point solutions won't cut it. Neither will siloed teams or 72-hour SLAs.

To defend against deception at scale, organizations need real-time, multi-channel, cross-surface, campaign-level visibility. That's what Social Engineering Defense delivers.

The question in 2025 isn't whether you're being targeted, it's whether you can see the attack before the damage is done.

About Doppel

We are on a mission to protect humanity from adaptive, AI-assisted social engineering. By creating the foundational system for ingesting all online data, our platform enables organizations to rapidly detect and disrupt cybercrime.

Doppel