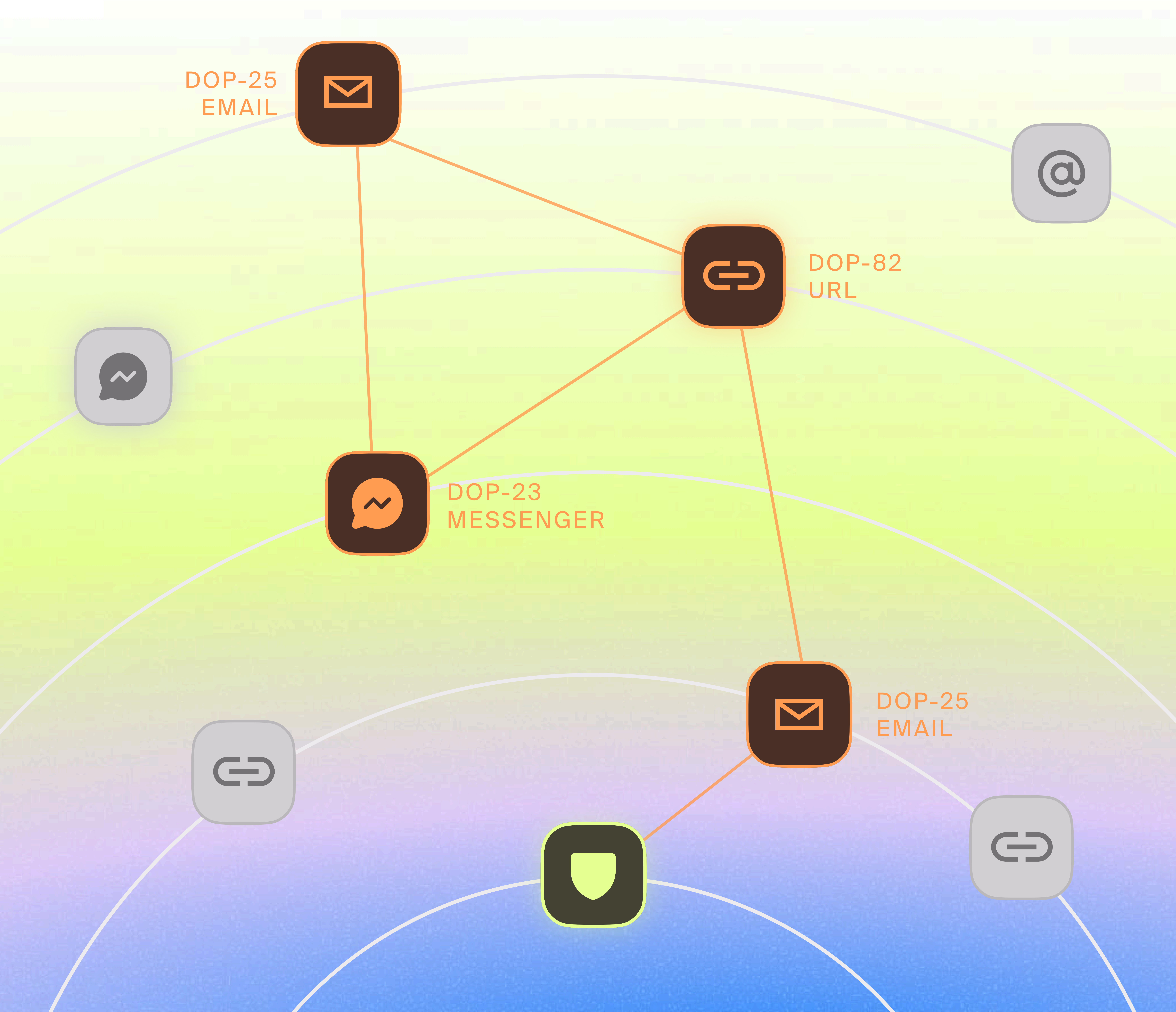
Doppel

A strategic framework
for modern threat disruption

Defining the Next Era of Cybersecurity:

The Case for Social Engineering Defense (SED)



Executive Summary

Social engineering isn't just a tactic anymore—it's the dominant operating model of modern cybercrime.

Supercharged by generative AI, today's adversaries don't break in. They log in. They impersonate. They build trust to deceive at scale. Deepfakes. Cross-channel manipulation. Scams that move laterally across platforms—they don't target infrastructure first, they target people.

Social engineering is a business risk with enterprise-wide reach. It compromises employees with spearfishing. It hijacks accounts through credential theft. It targets executives with impersonation, exposure, personal risk, and reputational damage. It deceives customers, eroding trust in your brand. And it exposes the entire organization to fraud, breach, regulatory scrutiny, and revenue loss.

Most security tools weren't built for this. They chase signals. They flag artifacts. But they don't touch the underlying infrastructure. They don't prevent a breach from happening in the future. And they don't tell you where the next attack will take hold.

That's why Social Engineering Defense (SED) is more than a framework—it's a strategic shift for cybersecurity leaders. SED moves security from reactive to proactive resilience and real-time disruption. It reframes the mission: no longer investigating attacks, but interfering with the systems that make them possible.

©2026 DOPPEL INC.

The Business Impact of Social Engineering Attacks

Social engineering exploits the most foundational asset in digital life: trust. The consequences are measurable, immediate, and enterprise-wide.

IMPACTS

$1.6 million per incident—the real price of a breach

From fraud losses to operational disruption, a single successful social engineering attack costs companies an average of $1.6 million.

- EXECUTIVES
- EMPLOYEES

Breaches start with a lie

Malware is out. Manipulation is in. Adversaries now gain access through impersonation—stealing credentials and trust, not just data.

- EXECUTIVES
- EMPLOYEES
- CONSUMERS

Brand damage that sticks

Customers don’t blame the scammer—they blame you. One fake site or impersonated account can undo years of trust in a single click.

- EXECUTIVES
- EMPLOYEES
- CONSUMERS

Compliance risk rising

AI-powered deception is a legal liability. Deepfakes, identity misuse, and synthetic fraud are drawing global regulatory scrutiny—and steep consequences.

- EXECUTIVES
- EMPLOYEES
- CONSUMERS

Fraud that scales faster than you can react

Fake profiles, spoofed ads, and scam content persist for weeks. And they don’t stop until the infrastructure behind them is dismantled.

- EXECUTIVES
- EMPLOYEES
- CONSUMERS

STAKEHOLDER	WHAT’S AT STAKE BEYOND OPERATIONAL DISRUPTION AND COMPLIANCE RISK
EXECUTIVES	Revenue loss, targeted impersonation, reputational and physical harm, liability
EMPLOYEES	Phishing, credential theft, insider exploitation
CONSUMERS	Scam exposure, trust erosion, brand disloyalty

©2026 DOPPEL INC.

Why Traditional Security Falls Short

Cybersecurity infrastructure wasn't built for deception at scale. And it shows. Today's attackers move like marketers: cross-channel, AI-powered, and built for speed. Meanwhile, most organizations are stuck with security stacks designed for malware, not manipulation.

HERE'S THE DISCONNECT:

Social engineering is dynamic.

Attackers shift tactics, platforms, and personas in real time.

Traditional security is still built for static threats.

Even with AI bolted on, legacy tools depend on slow, siloed workflows and outdated infrastructure.

The gap isn't closing. It's compounding.

As attackers get faster and more adaptive, security stacks that weren't built for deception fall further behind—no matter how much intelligence they ingest.

Enterprise

SECURITY LIMITATION	WHY IT FAILS
Still stuck in the inbox	Most security stacks treat social engineering as a phishing problem. That ignores impersonation across LinkedIn, WhatsApp, Telegram, TikTok, and encrypted platforms.
Signal without action	Threat intel platforms surface indicators, but leave remediation to overloaded teams. Insight ≠ protection if it doesn't lead to takedown.
Vanity metrics create blindspots	Email click rates alone do not accurately reflect the risk posed by phishing attacks that span channels with unprecedented personalization and sophistication.
Too much manual, too little momentum	SOC workflows depend on human triage while attackers pivot in real time, outpacing legacy response cycles.
Static templates create stale defenses	Generic simulation templates and training content fall short when it comes to preparing employees against modern social engineering attacks.
Blind to attacker infrastructure	Traditional tools flag domains or emails individually but miss how assets connect into full attacker ecosystems.
Detection doesn't scale. Adversaries do.	Delayed action, fragmented visibility, and repeat attacks under new names. It's whac-a-mole at enterprise scale.

©2026 DOPPEL INC.

Digital Risk Protection (DRP)

SECURITY LIMITATION	WHY IT FAILS
Point solutions, not platforms	DRP tools flag & remove symptoms—domains, fake sites, spoofed accounts—but can't correlate or dismantle full infrastructure.
Slow, surface-level takedowns	Manual takedown workflows can't keep up with fast-moving, multi-platform campaigns.
No cross-channel correlation	DRP tools track assets, not attacker behavior. When a scam shifts platforms, DRP loses the thread.
Limited visibility, limited impact	DRP doesn't touch encrypted apps, fringe networks, or user-submitted signals. It can't turn reports into disruption.

Human Risk Management (HRM)

SECURITY LIMITATION	WHY IT FAILS
Traditional simulations don't cut it	Simulations that focus only on email and use static templates don't reflect modern attacker behavior, in which multi-step attacks are carried out across every channel.
Modern attacks demand modern training	Legacy SAT vendors offer outdated, overly simplified training video libraries that satisfy compliance checkboxes but fail to impact meaningful behavior change.
Click rates are dead	Email click rates alone do not provide accurate insight into an organization's risk surface, because not every click is created equal.
Compliance checkboxes don't reduce risk	Traditional awareness training and generic email simulations check compliance boxes, but overlook serious gaps in security. By relying on topline metrics, dated training, and bare-bones testing, organizations cannot accurately measure risk in their organization or eliminate weak spots.

Why This Matters Now

Social engineering isn't new, but the scale, speed, and sophistication of today's campaigns demand a reset. Emerging channels, synthetic media, and AI-driven deception have created a threat landscape where:

- Brand damage happens before alerts fire.
- Executives are impersonated before detection tools engage.
- Employees are exploited without even knowing it.
- Consumers are deceived before DRP can act.

And with every passing day, the attacker's playbook continues to evolve, maximizing ROI and skating by undetected. The longer you rely on outdated tools to fight modern threats, the more expensive, and risky, the gap becomes. Social Engineering Defense isn't a nice-to-have. It's a strategic imperative for protecting your people, your brand, and your bottom line.

Introducing the Social Engineering Defense (SED) Framework

SED redefines what effective cyber defense looks like in the age of AI-powered impersonation. It's not a tool or a tactic—it's a strategic orientation. A blueprint for turning detection and disruption into prevention. It's built around three foundational capabilities:

01

Networked Intelligence: The Compounding Advantage of Shared Defense

A networked model flips the script, turning every defense into a shared advantage.

WHAT IT IS

Networked intelligence is the foundation of scalable, collaborative security. It's a shared threat model that continuously maps attacker infrastructure—linking domains, phone numbers, spoofed accounts, scam content, and dark web assets into a unified, always-evolving threat graph.

This intelligence then powers threat-informed phishing simulations and training content to arm employees against the attacks actually happening in the wild. So if your CFO is targeted on Monday, the threat is mitigated within hours, and your entire team is trained by Tuesday.

Every report, every signal, every takedown contributes to the whole, making detection faster, disruptions smarter, and defenses stronger across the board.

WHY IT MATTERS

Adversaries don't work in silos. They reuse infrastructure and recycle tactics across victims, industries, and regions. Without a networked approach, defenders are left solving the same problem repeatedly, learning in isolation while attackers operate at scale.

STRATEGIC OUTCOMES

- Faster detection and response through shared signal correlation
- A system that learns continuously, and acts collectively
- Threat-informed phishing simulations and training content
- Reduced attacker ROI through infrastructure reuse penalties
- OSINT-backed HRM campaign recommendations
- Pattern recognition across enterprises and platforms
- Disruption driven by context, not just content
- One-click threat-to-simulation cloning

©2026 DOPPEL INC.

02

Multimodal, Multi-Channel Defense: Protecting Against Threats Across Any Format or Channel

To counter dynamic threats, defenses must be fluid, contextual, and format-independent.

WHAT IT IS

Modern social engineering attacks are not bound to a single vector or channel. A true SED framework leverages AI that spans formats, including voice, video, and text, and acts across channels, including mainstream and emerging platforms. Detections must go beyond scanning for keywords or static indicators. Modern SED involves analyzing patterns across modalities and platforms, detecting intent and manipulation wherever it occurs, and automating takedowns across every vector.

But taking down threats across channels isn't enough: teams must also simulate multi-channel social engineering attacks (across email, SMS, Telegram, and voice) to measure how employees and BPOs (i.e. outsourced helpdesks) actually detect, report, and respond to threat-informed campaigns.

WHY IT MATTERS

Social engineering is inherently dynamic. Attackers pivot quickly from spoofed emails to deepfakes, from fake voice calls to cloned social profiles—often within the same campaign. A defense framework that's not modality-agnostic and channel-aware will always fall behind. Traditional defenses fail because they're built for isolated channels and fixed formats.

Social Engineering Defense demands real-time visibility into diverse threat vectors, even where traditional tools have blind spots, and multi-channel simulations & training.

STRATEGIC OUTCOMES

- Recognition of synthetic content and AI-generated impersonation across formats
- Visibility into impersonations across non-traditional and emerging platformS
- Reduced attacker dwell time through cross-channel intelligence linkage
- Detection driven by behavioral context, not just static signatures
- Proactive coaching and defanged simulations that mirror attacker TTPs
- Ability to identify and eliminate vulnerabilities on specific channels
- Channel-specific training and simulations
- Build resilience across every channel

©2026 DOPPEL INC.

03

Agentic AI Automation: Turning Scale Into a Liability

Scalability is the attacker's advantage. Automation is how defenders take it away.

WHAT IT IS

A key principle of Social Engineering Defense is automated disruption – identifying, dismantling, and building resilience against the domains, phishing kits, fake accounts, and scam infrastructure that power impersonation at scale. This isn't about chasing artifacts. It's about removing the machinery behind the attack.

WHY IT MATTERS

Automated graph analysis and bulk takedowns let teams protect more brands, executives, and assets—without adding new analysts or drowning in manual triage.

Agentic AI automation also makes it easy to generate and run sophisticated, multi-step simulation and training campaigns that protect against the latest attacker tactics, through vibe phishing simulations and AI-generated custom training content. Detection alone isn't defense. Without strong defenses, social engineering remains cheap, repeatable, and profitable. But when infrastructure is removed quickly, teams are trained in resilience, and attempts are repeatedly thwarted, operating and sustaining it becomes expensive.

STRATEGIC OUTCOMES

- Real-time disruption across social, web, messaging, and fringe platforms
- Faster response cycles without expanding analyst workloads
- Automated takedown of attacker ecosystems, not just individual assets
- Identify and remediate weak spots with scalable red teaming
- Increased operational cost for adversaries reliant on reuse and scale
- Easily create sophisticated phishing simulations to validate readiness
- Reduced attacker dwell time and repeat threat reappearance
- Automate custom training content creation for tailored learning

©2026 DOPPEL INC.

The Future is Disruption-Driven Defense

Social engineering attacks are easy to launch, difficult to detect, and increasingly costly to contain—unless you dismantle the business model behind them.

Social Engineering Defense isn't an upgrade to traditional security; it's a strategic realignment—one that shifts focus from reacting to threats to eliminating the systems that make them possible.

ORGANIZATIONS THAT EMBRACE SED CAN

- Disrupt threats before they spread
- Correlate weak signals into strong action
- Match attacker speed without scaling headcount
- Identify & eliminate weak spots
- Improve internal readiness
- Increase operational efficiency

This is more than a response. It's a reset. From alert fatigue to active disruption. From repetitive training to behavior shaping. From symptom chasing to source removal. From vanity metrics to actionable insights.

The Time to Detect is Shrinking.

The Time to Disrupt is Now.

Every security leader must ask:
Is our organization built to detect deception, or dismantle it? Let's talk.

Book Your Demo at

www.doppel.com/request-a-demo