Doppel

# Why Manufacturers Choose Doppel

## Defending against modern social engineering attacks

## A New Risk Reality

Manufacturers are facing a fundamental shift: social engineering is becoming one of the fastest growing drivers of operational disruption, supply chain compromise, intellectual property theft, and financial fraud. Manufacturing is the most targeted industry for the fifth consecutive year. (IBM)

As manufacturers digitize operations and expand connectivity across suppliers, contractors, IT systems, and operational technology (OT) environments, attackers are exploiting trust at every level of the business.

Using AI-generated content, deepfakes, spoofed identities, and coordinated impersonation campaigns, threat actors target employees, executives, procurement teams, suppliers, and partners with unprecedented speed and scale.

These attacks are no longer isolated incidents. They are coordinated campaigns spanning email, domains, social media, messaging platforms, voice channels, and third-party ecosystems.

Doppel exposes risks and eliminates threats across every digital channel before attacks impact your operations, workforce, supply chain, intellectual property, or revenue.

## Key Threats Facing Manufacturers

### Executive & Vendor Impersonation

AI-generated messages, deepfakes, and spoofed identities used to impersonate executives, procurement teams, suppliers, and logistics partners to authorize fraudulent payments, redirect shipments, and manipulate business processes.

### Helpdesk & Operational Support Attacks

Threat actors target IT helpdesks, plant floor support teams, and operational personnel through vishing and social engineering to gain access to critical systems and environments.

### Business Email Compromise & Credential Theft

Lookalike domains, fake vendor portals, and phishing campaigns are designed to compromise employee credentials and enable unauthorized access to business and operational systems.

### Supply Chain & Third Party Fraud

Fraudulent supplier communications, counterfeit procurement portals, and partner impersonation campaigns introduce risk across complex vendor ecosystems.

### Intellectual Property & Data Exposure

Leaked proprietary designs, engineering documentation, trade secrets, and employee credentials fuel espionage, fraud, and downstream compromise.

# Doppel for Manufacturing: A Unified Defense Platform

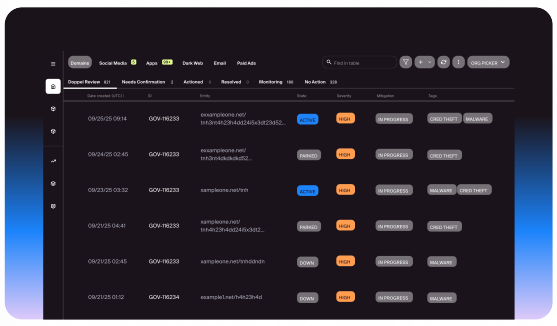
Traditional security tools are effective against technical threats, but struggle to stop AI-driven social engineering attacks that exploit human trust, business processes, and supplier relationships.

Attackers operate across email, domains, voice, social media, messaging platforms, and third-party ecosystems, while traditional tools remain siloed, reactive, and disconnected.

Doppel unifies detection, disruption, training, simulation, and email security into a single platform, helping manufacturers identify and eliminate coordinated, multi-channel attack campaigns before they impact production, operations, suppliers, or revenue.

---

## Brand Protection



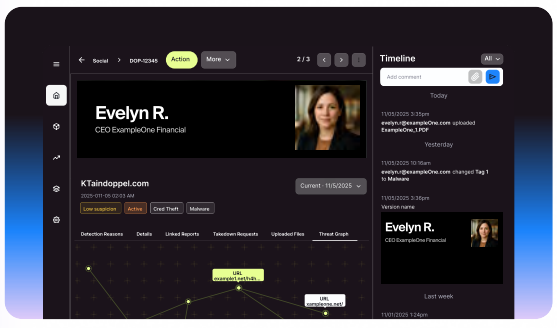
Doppel autonomously detects and dismantles impersonation and fraud targeting your organization across:

- **Fraudulent supplier and procurement portals**
- **Lookalike domains and spoofed websites**
- **Social media impersonation and messaging scams**
- **Malicious paid advertisements and counterfeit digital assets**

Doppel shuts down fraudulent experiences before employees, suppliers, or customers interact with them, reducing operational risk and protecting trusted business relationships. By eliminating attacks at the source, manufacturers can reduce exposure to vendor fraud, supply chain compromise, and brand abuse.

---

## Executive Protection

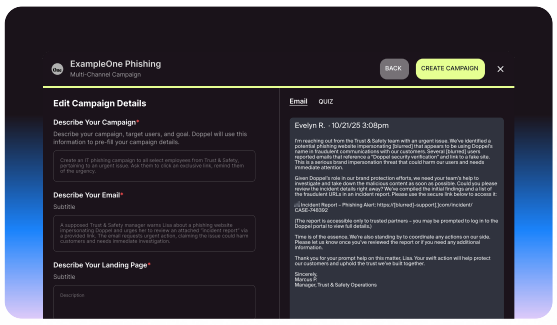



Manufacturing executives and operational leaders are increasingly targeted by sophisticated social engineering campaigns. Doppel protects executives and leadership teams from:

- **AI-generated impersonation and deepfake-enabled fraud**
- **Targeted vishing and social engineering attacks**
- **Exposure of personal and professional information used to facilitate doxxing or compromise**

Doppel reduces the risk of fraudulent payments, supplier manipulation, and high-impact social engineering attacks targeting leadership. This is critical for maintaining trusted supplier relationships, and minimizing financial and reputational damage tied to executive compromise.

## Simulation

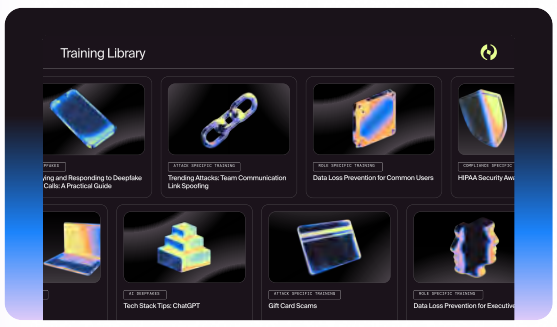



Doppel simulates live attack scenarios across channels to identify internal breakdowns before attackers exploit them:

- **Multi-channel simulations across phishing, vishing, smishing, and messaging attacks**
- **Threat-informed campaigns modeled on supplier fraud, procurement scams, executive impersonation, and operational social engineering attacks**
- **Agentic AI-driven scenarios tailored to procurement, helpdesk, IT, OT, and plant operations teams**

Doppel provides a safe environment to validate defenses, identify process vulnerabilities, and improve resilience across critical operational workflows. By exposing gaps in identity verification, approval processes, and supplier communications, manufacturers can reduce the risk of operational disruption, vendor fraud, and supply chain compromise.

## Security Awareness Training

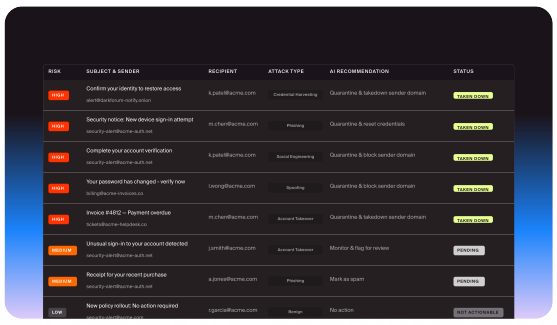



Traditional awareness programs fail because they are static and disconnected from the real threats targeting manufacturing organizations. Doppel delivers targeted, role-specific training built from actual attack activity targeting your organization:

- **Deepfake-driven content featuring your executives, suppliers, and operational workflows**
- **Automated training programs for onboarding and continuous reinforcement**
- **Personalized coaching with real-time feedback to improve decision-making and reporting**

Doppel transforms awareness into measurable behavior change by aligning training directly with real attack tactics targeting manufacturing environments. Employees become more effective at recognizing vendor fraud, impersonation attempts, phishing campaigns, and operational social engineering attacks before they lead to disruption.

## Email Security




Most email security solutions focus on detecting and removing malicious messages from the inbox. Doppel Email Security detects phishing, business email compromise, impersonation, and social engineering attacks while connecting every message to the infrastructure behind it:

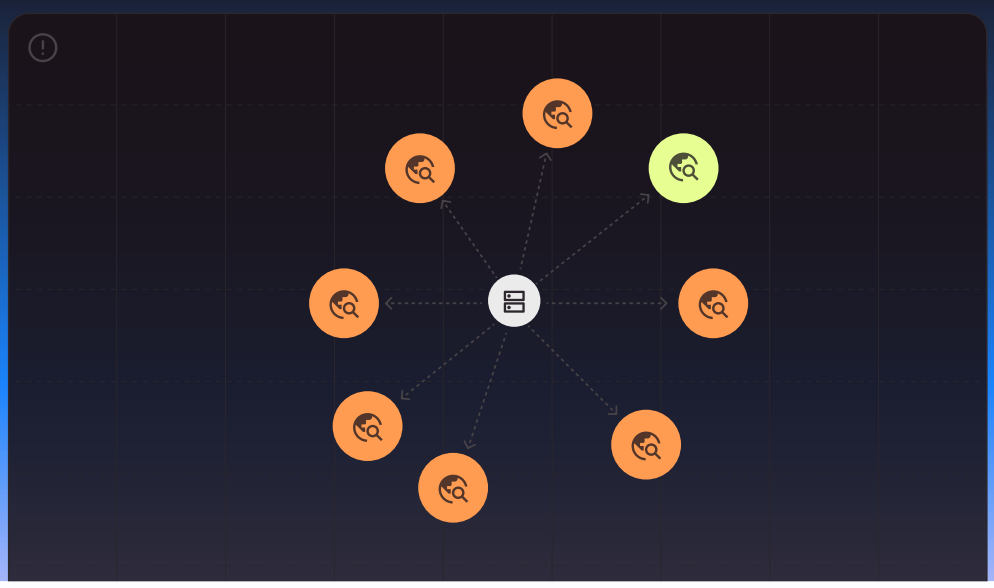
- **Agentic detection powered by natural language policies rather than static rules or black-box models**
- **External attack infrastructure intelligence that maps domains, impersonation assets, and attacker networks**
- **Machine-speed disruption of underlying malicious infrastructure at the source**

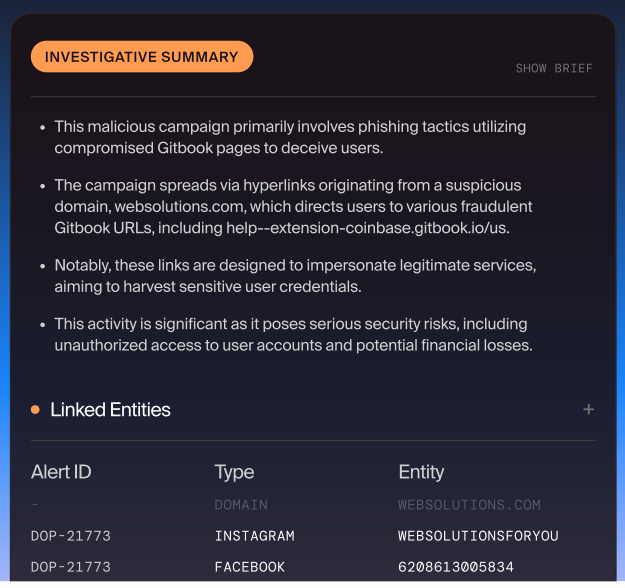
Doppel goes beyond inbox protection by disrupting the campaigns behind phishing and impersonation attacks. Manufacturers can stop attacks at the inbox while dismantling the cross-channel infrastructure used to target employees, suppliers, and partners.

## Threat Graph Intelligence

Doppel connects signals across email, domains, voice, social media, messaging platforms, procurement ecosystems, supplier networks, and more to uncover coordinated campaigns targeting your organization.

Doppel's Threat Graph maps attacker infrastructure, identities, and behaviors into a complete view of the campaign, revealing how seemingly isolated threats are connected. This allows Doppel to disrupt the entire operation, not just individual assets, forcing threat actors to rebuild attack infrastructure instead of simply replacing a single phishing page or fake account. By changing the economics, Doppel increases adversary cost, reduces attacker ROI, and makes future threat campaigns significantly harder to execute.





## How Doppel Protects Manufacturing Organizations

Manufacturers face growing risk from impersonation, supply chain fraud, business email compromise, and social engineering attacks targeting employees, executives, suppliers, and operational teams.

By partnering with Doppel, organizations move from reactive investigation and manual response to proactive risk reduction through AI-driven threat detection, disruption, simulation, and training across email, domains, social media, messaging platforms, and the dark web.

Doppel helps manufacturers identify and eliminate external threats while building a workforce that can recognize and stop attacks before they impact operations.

Manufacturers use Doppel to:

- Prevent operational disruption before it impacts production
- Stop vendor impersonation before funds are transferred or access is granted
- Protect intellectual property and proprietary documentation
- Protect employee inboxes from phishing, business email compromise, and impersonation attacks
- Reduce credential theft and account compromise
- Strengthen supplier trust and supply chain resilience
- Cut through alert noise and reduce investigation effort
- Build employee resilience through realistic phishing, vishing, and social engineering simulations
- Strengthen readiness for NIST CSF 2.0, IEC 62443, and other industry-specific regulatory requirements
- Deliver targeted training tailored to procurement, IT, OT, helpdesk, and operational teams

---

## The Bottom Line

Manufacturers are increasingly targeted by AI-powered impersonation, vendor fraud, phishing, business email compromise, and social engineering attacks designed to disrupt operations and exploit trusted relationships.

Doppel gives manufacturing organizations the ability to identify coordinated threats, stop them early, and build resilience across employees, suppliers, executives, and critical business processes.