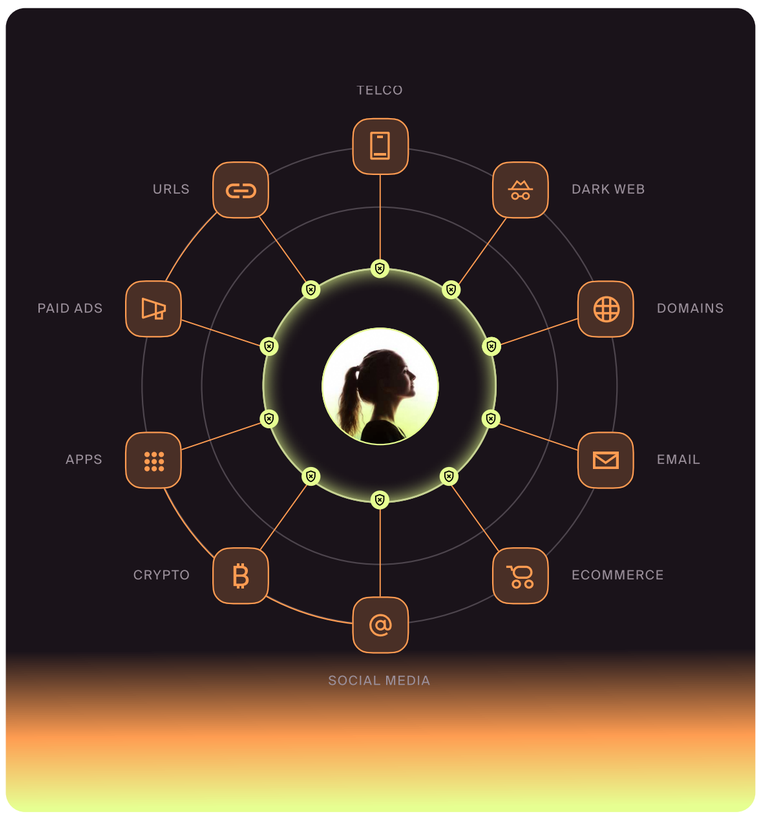
Doppel

MANUFACTURING SERVICES

Social Engineering in Manufacturing

Protecting your operations, supply chain, IP, and revenue from AI-driven fraud & attacks

The growing attack surface



In manufacturing, operational continuity, trusted supplier relationships, and workforce resilience are critical to business success. They are also prime targets for attackers.

As manufacturers digitize operations and expand connectivity across suppliers, contractors, IT systems, and operational technology (OT) environments, the attack surface continues to grow. Threat actors are exploiting this shift with sophisticated impersonation and social engineering attacks targeting employees, executives, vendors, and partners.

These attacks are no longer isolated. They are coordinated, persistent, and built to scale, spanning domains, email, social media, messaging platforms, procurement portals, voice calls, and supplier ecosystems.

Using AI-generated content, deepfakes, and spoofed identities, attackers create highly convincing interactions that exploit trust with unmatched speed and scale. What once took days or weeks can now be executed in minutes.

External threats do not stay external. They lead to:

- Operational disruption and production downtime
- Fraudulent payments and business email compromise
- Supply chain compromise and vendor fraud
- Intellectual property theft and data exposure
- Loss of partner trust and brand reputation damage
- Increased cybersecurity and compliance risk

Threats to Manufacturers

- **Helpdesk and Contact Center Vulnerability:** Manufacturing and engineering organizations have the highest vishing vulnerability rate of any industry. A single call to an IT helpdesk, plant floor contact, or support function can provide attackers with access to critical systems and operations.
- **Executive and Vendor Impersonation:** AI-generated messages, deepfakes, and spoofed identities are used to impersonate executives, procurement teams, suppliers, and logistics partners to authorize fraudulent transfers, redirect payments, and manipulate business processes.
- **Business Email Compromise and Phishing:** Lookalike domains, fake vendor portals, and targeted phishing emails compromise employee credentials, enabling account takeover and unauthorized access to business and operational systems.
- **Supply Chain and Third Party Fraud:** Fraudulent supplier communications, counterfeit procurement portals, and impersonation of trusted partners introduce risk across complex vendor ecosystems and increase the likelihood of operational disruption.
- **Intellectual Property and Data Exposure:** Leaked proprietary designs, trade secrets, engineering documentation, and employee credentials circulate across the open and dark web, fueling espionage, fraud, and downstream compromise.

27.7%

of all cyber incidents targeted manufacturing, making it the most attacked industry for the fifth consecutive year

SOURCE: IBM X FORCE THREAT INTELLIGENCE INDEX 2026

60%

year over year increase in supply chain and third party involvement in breaches

SOURCE: 2026 VERIZON DBIR

91%

of manufacturing breaches were caused by system intrusion, social engineering, and basic web application attacks

SOURCE: 2026 VERIZON DBIR

19.2%

vishing vulnerability rate in manufacturing and engineering, the highest of any industry

SOURCE: 2024 KEEPNET VOICE PHISHING RESPONSE REPORT

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

MANUFACTURING SERVICES

Doppel

Where Existing Tools Fall Short

Most manufacturers already have multiple security tools in place, but those tools were not designed for modern social engineering attacks.

Fragmented visibility across security, IT, OT, procurement, legal, and risk teams forces analysts to manually correlate signals across channels while high alert volumes obscure real threats. As a result, detection and response are often reactive and slow, while traditional security awareness training frequently fails to reflect the real-world attack patterns targeting manufacturing environments.

Modern Threats Require Modern Solutions

Doppel defends against the full social engineering attack surface by unifying detection, correlation, disruption, simulation, training, and email security across email, domains, social media, messaging platforms, voice channels, procurement portals, and more.

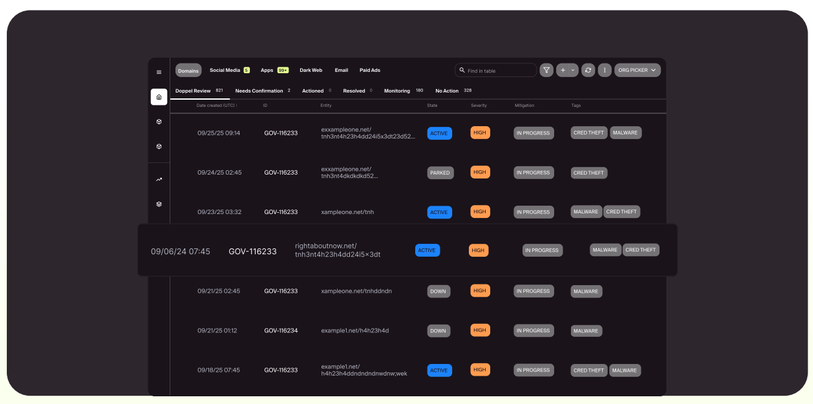
The platform identifies and prioritizes high-risk threats involving impersonation, credential theft, supply chain fraud, intellectual property exposure, and data leaks. By correlating signals across channels - including Microsoft 365 and Google Workspace - Doppel provides a single view of coordinated attack campaigns targeting operations, employees, vendors, and executives. Rather than addressing isolated incidents, Doppel disrupts the full attacker infrastructure.

Doppel also strengthens internal resilience through realistic vishing, smishing, and phishing simulations, role-specific security awareness training, and red teaming exercises tailored to manufacturing environments, helping reduce human risk and support compliance requirements.

With Doppel, manufacturers move from reactive response to proactive risk reduction:

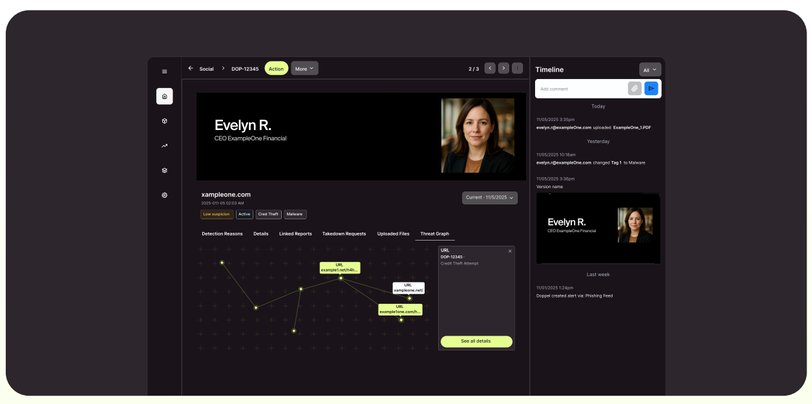
- Prevent operational disruption by reducing the risk of phishing, credential theft, social engineering, or vendor impersonation attacks before it impacts production or funds
- Protect employee inboxes, intellectual property, trade secrets, and proprietary documentation, and other sensitive business assets from phishing, business email compromise, impersonation, and data theft
- Cut through alert noise and reduce manual investigation effort
- Strengthen readiness for NIST CSF 2.0, IEC 62443, and other industry-specific regulatory requirements
- Simulate real world attacks against helpdesk, procurement, IT, OT, and plant floor teams
- Measure human risk and deliver targeted, role-specific training across identity verification and response workflows

Products Powered by the Doppel Platform



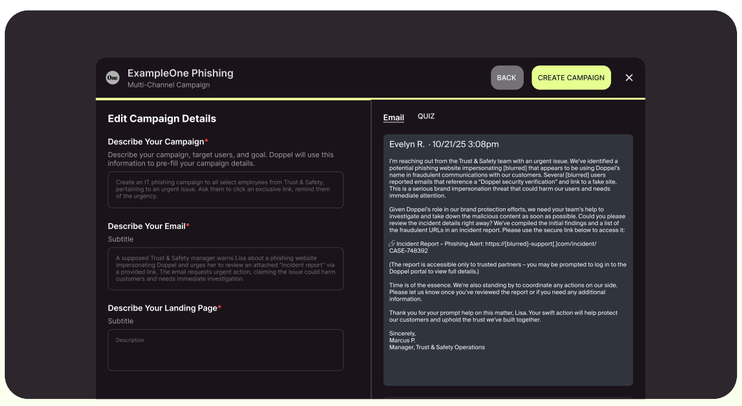
Brand Protection

Detect and remove impersonation, brand abuse, fraudulent supplier portals, and scams across domains, apps, social media, messaging platforms, and more.



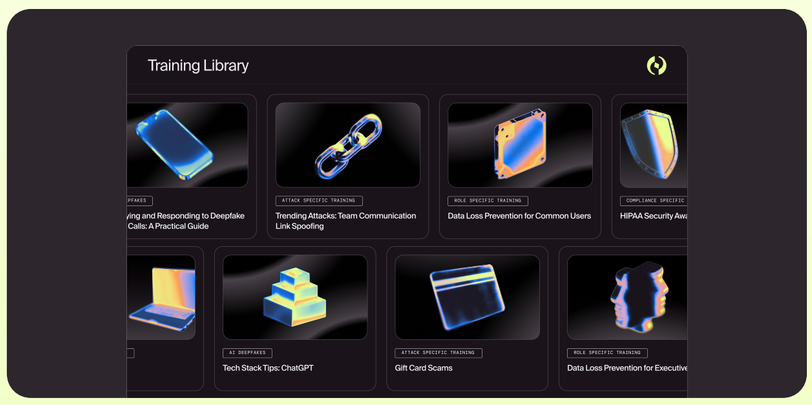
Executive Protection

Protect executives and leadership teams from impersonation, targeted social engineering attacks, and sensitive data exposure.



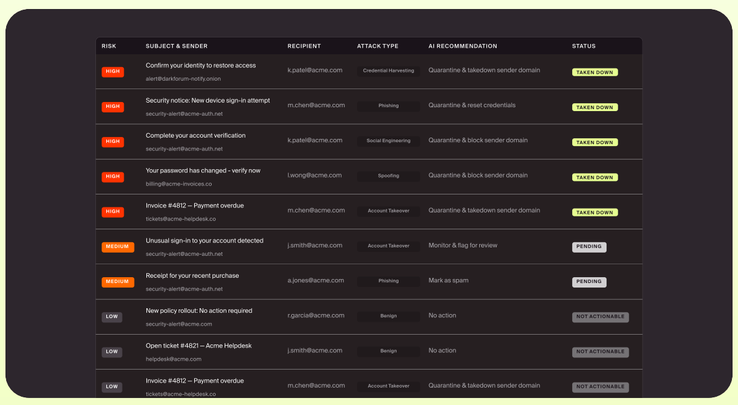
Simulation

Test employees, helpdesk agents, procurement teams, IT staff, and operational personnel against realistic vishing, smishing, and phishing scenarios across channels.



Security Awareness Training

Train employees to recognize and respond to modern, AI-driven, social engineering attacks tailored to manufacturing workflows, plant floor operations, and vendor communication processes.



Email Security

Automatically remediate phishing, business email compromise, and impersonation attacks in the inbox, mapping and dismantling the underlying attack infrastructure.

Book your demo at

doppel.com/request-a-demo