Doppel

OUTPACING WHAT'S NEXT
IN SOCIAL ENGINEERING

The Human Risk Management Blueprint

Your Fast-Track from Legacy Training
to AI-Native HRM

©2026 DOPPEL INC.

Social engineering is evolving faster than ever before.

Attackers are using AI to create sophisticated lures, realistic deepfakes, and multi-channel pretexts that bypass email filters and fool even recently-trained employees.

Table of Contents

Why the Compliance Checkbox isn't Enough

For decades, the security industry has treated humans as the first (and often last) line of defense against threats. They've been trained through annual videos and predictable phishing test emails.

This approach has failed.

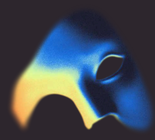
According to the Verizon 2025 Data Breach Investigations Report, over 60% of breaches still involve the human element.[1] Why? Attackers have upgraded to machine speed, but defense remains stuck in a manual past.

Human Risk Management (HRM) represents a fundamental category shift. Analysts such as Forrester[2] recognize HRM as a new market category that moves away from measuring compliance toward measuring and modifying behavior.

[1] 2025 Data Breach Investigations Report
[2] The Future Is Now: Introducing Human Risk Management

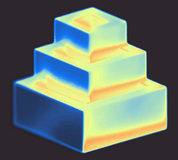
Read on for a roadmap for shifting from checkbox compliance to active human risk management.

We'll explore:



The mechanics of AI-native deception

The failure of click rates as a metric



A 3-pillar approach to simulation, training, and risk modeling

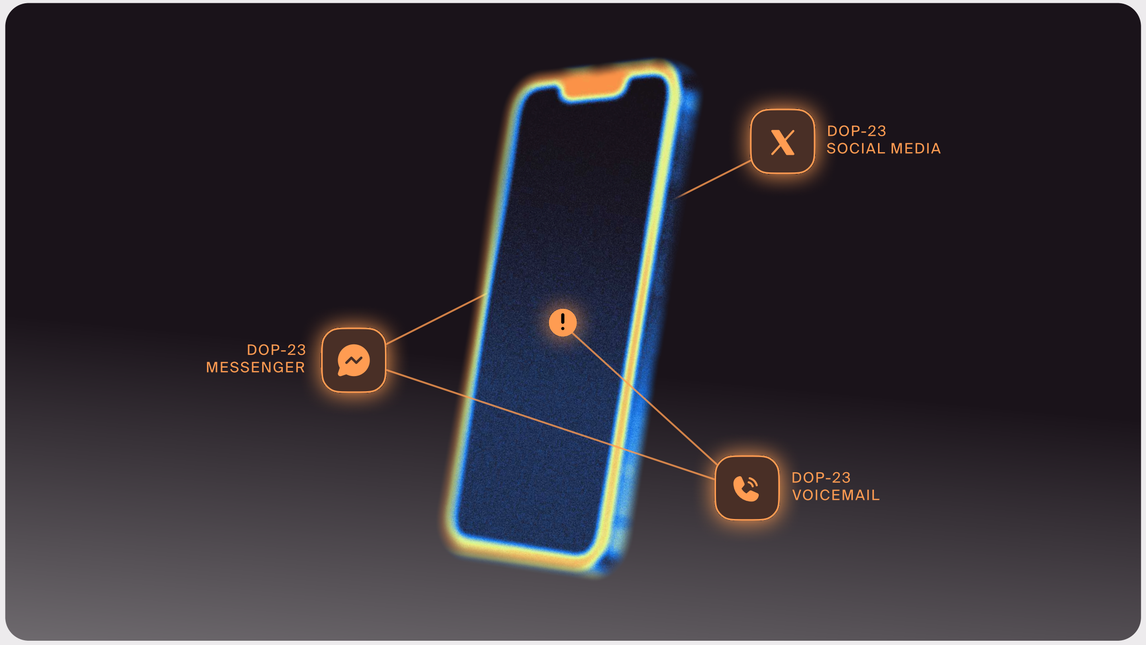
We'll conclude with a tactical framework for migrating your defense from legacy tools to measurable, agentic resilience.

The AI Inflection Point

The hard truth is that attackers are using AI to deceive at machine speed, and their approaches are far more advanced and harder to flag than what security teams have prepared for.

> Generative AI has moved us away from defending against "foreign royalty" asking for millions and gift cards.

Now, we're defending against Scattered Spider-style adversaries who use agentic AI to conduct hyper-personalized, multi-channel campaigns.



How a 6-Minute Call Cost $100 Million

High-profile breaches at MGM Resorts[3] and Clorox[4] weren't the result of zero-day exploits or complex code. They came down to a perfectly executed phone call.

Attackers from the group Scattered Spider used a simple, effective loop:

This is why email-only training isn't enough.

Doppel's Helpdesk Mode mirrors this exact threat. Our vishing agents can navigate IVR phone trees and engage helpdesk staff in live, multi-step conversations to ensure your frontline doesn't become your front door for the next major breach.

[3] MGM Resorts breached by 'Scattered Spider' hackers: sources

[4] Clorox Reels After Cyberattack Woes Spur Analysts to Sour on Shares

Here's the scope of the crisis across three domains:

Volume

AI has fundamentally changed the economics of social engineering. Attackers have increased phishing volume by over 1,000% while their own costs have dropped by 95%.[5] More volume also means a bigger financial catastrophe, with the average cost of a social engineering breach hitting $4.4 million.[6] Deloitte projects that GenAI-enabled fraud could cost the U.S. $40 billion by 2027.[7]

Variety

Attacks are no longer siloed in the inbox. The industry has seen a 442%[8] increase in vishing (voice phishing), and over 41%[9] of attacks now jump between channels (SMS, Telegram, Teams). Because email-only security tools can't see these other platforms, they leave critical blind spots that agentic AI is designed to exploit.

Velocity

Attackers now operate at machine speed, while traditional defense remains stuck in a manual past. The median time for a user to click a malicious link is 21 seconds. The median time to surrender credentials is 28 seconds. Your organization has a window of less than 60 seconds before a breach occurs.[10]

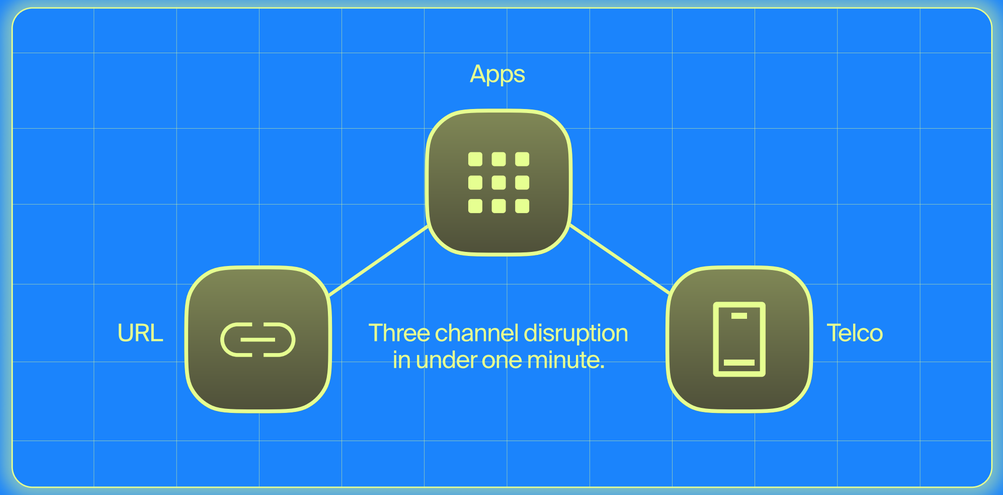
Legacy vendors can now attack more companies than ever, and with more precision, thanks to AI.

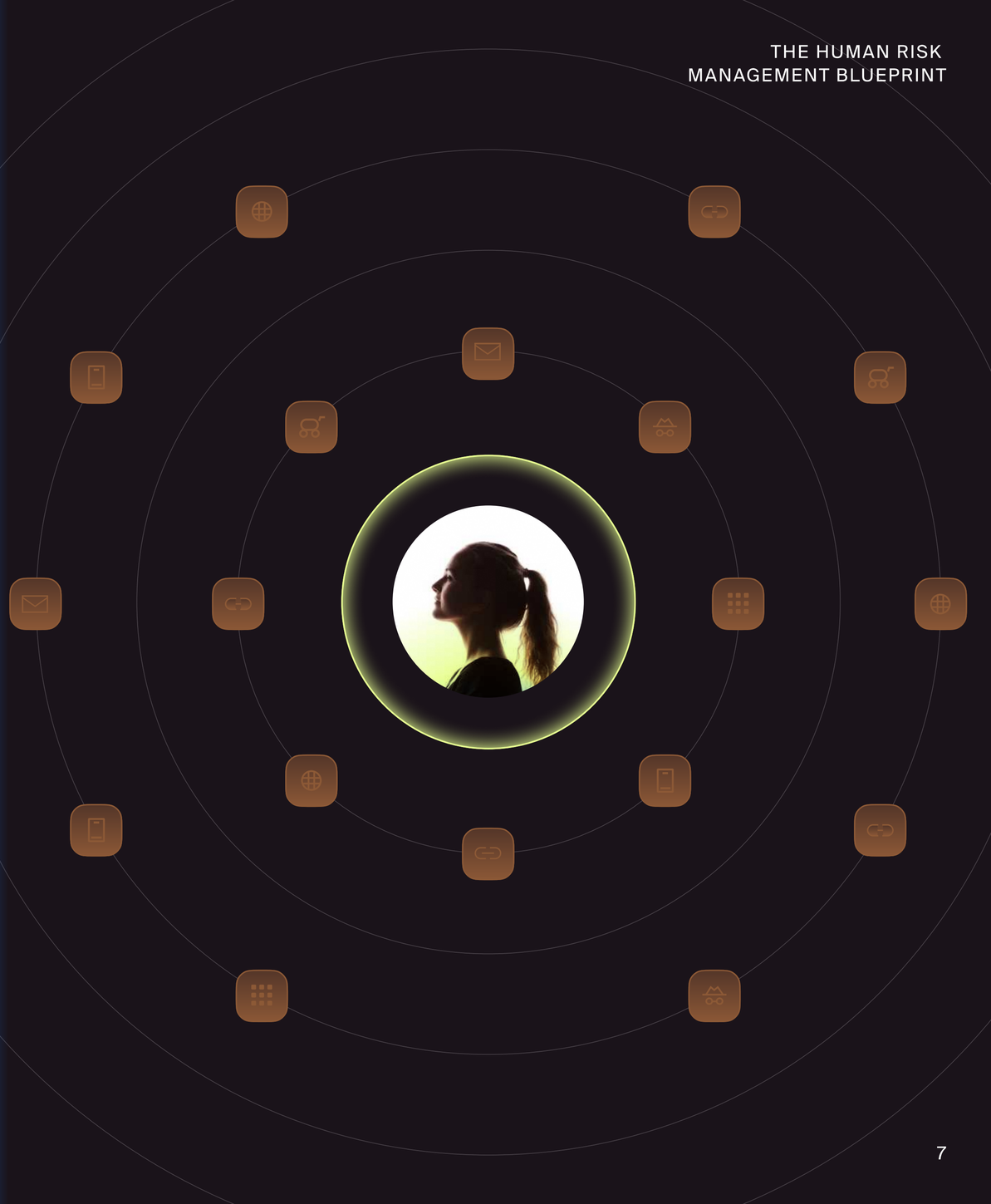
[5] Gartner Survey Reveals GenAI Attacks Are on the Rise
[6] Cost of a Data Breach Report 2025
[7] Generative AI is expected to magnify the risk of deepfakes and other fraud in banking
[8] 2025 CrowdStrike Global Threat Report
[9] Phishing Attack Statistics 2026
[10] 2024 Data Breach Investigations Report

THE BOTTOM LINE

It’s not enough to know who clicked on a malicious link.

With the rise of AI-powered attacks, you need to focus on how quickly you can detect, disrupt, and train against an attack that spans three channels in under a minute.





CHAPTER 2

Why Click Rates are Dead

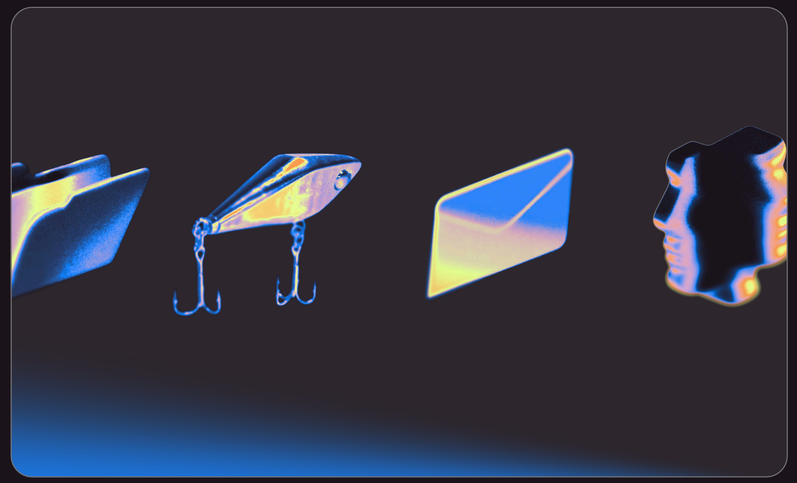
The most misleading metric in security today is a low click rate. It creates a false sense of security while ignoring the reality of privileged access.

In the past, organizations viewed a 1.5% click rate as a success. However, HRM recognizes that not all clicks are created equal.

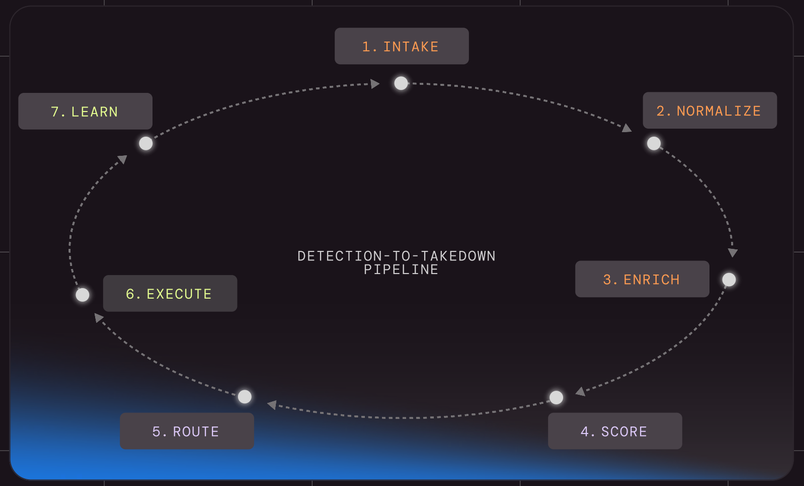
Here are a few examples.

First, there's the high-risk user. A click from a DevOps engineer with root access to production is many times more dangerous than a click from a marketing intern with access to a design tool.

There's also the issue of the "reporting multiplier." The goal is not just to stop clicks. It's to increase reporting. Users with modern training report simulated attacks 4 times more frequently.
In HRM, the Reporting Rate is a much more accurate predictor of resilience than the click rate.



Doppel HRM replaces static spreadsheets with Dynamic Risk Modeling, correlating user behavior, access levels, and threat exposure into a single, actionable score.



THE BOTTOM LINE

Reporting click rates alone is not a sufficient measure of resilience.

21s

Median time for a user to fall for a malicious link

28s

Median time for a user to surrender credentials[11]

Resilience is measured by how quickly your workforce flags a threat, not by the absence of a click.

Start reporting the percentage of privileged access you've protected and your mean time to report.

[11] Version Business Report: 2024 Data Breach Investigations Report

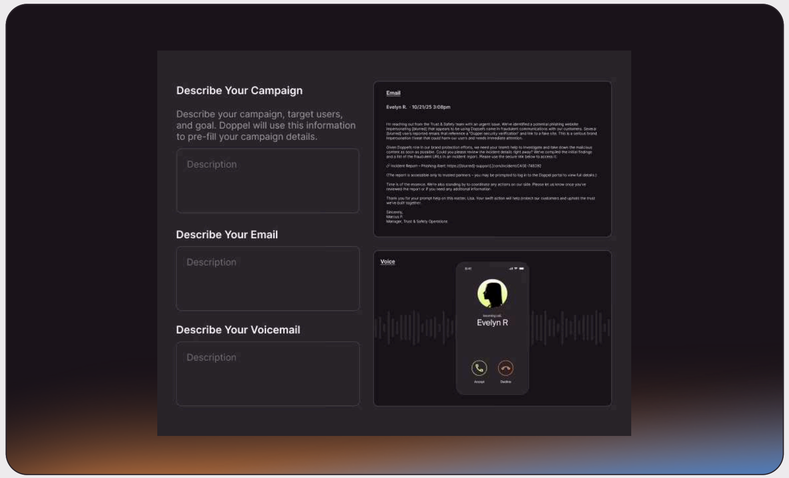
The 3 Pillars of the Doppel Difference

Simulation, Training, and Risk Modeling

To bridge the gap between where legacy vendors stop and what the industry actually needs, Doppel HRM integrates 3 core products into a single intelligence-backed cycle.

1. Simulation: The Agentic Offensive

Doppel Simulation doesn't use static templates. It uses Agentic AI and the Doppel Threat Graph to simulate real-world phishing attacks across channels.



- **Multi-step Conversational Threading:** Our AI agents engage in back-and-forth exchanges across email, voice, SMS, business communication tools (Zoom and Microsoft Teams), and Telegram, and chain multiple channels together to emulate actual attacker tactics.

- **Threat Cloning and Social Engineering Advisories**: We convert live threats detected by our Digital Risk Protection (DRP) solution into simulations with a single click, so employees are tested against the tactics that attackers are using in the wild. Doppel's Threat Graph Intelligence also powers proactive advisories that recommend training content and simulations based on actual attacker campaigns targeting your industry or employees.

- **Vishing and BPO Testing**: We can conduct up to 200,000 deepfake voice calls per week, navigating IVR phone trees to test the resilience of your helpdesk or contact center and give you insight into where protocols break down.

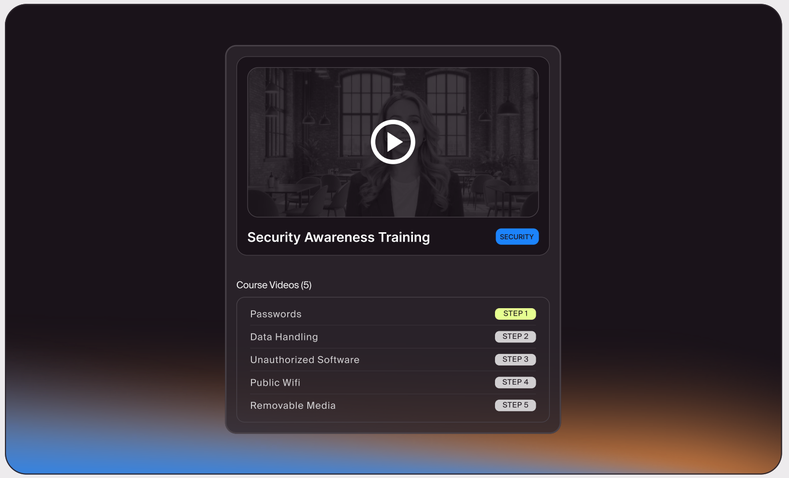
2. SAT: Next-Gen Awareness and Training

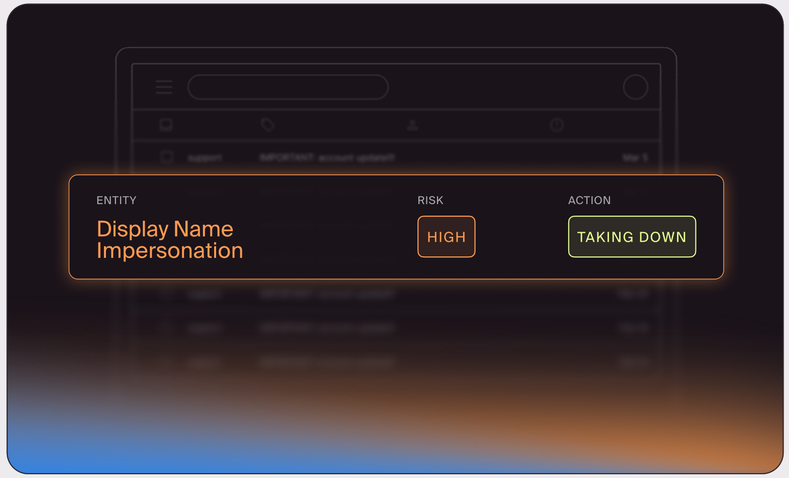
Legacy video libraries are generic and boring. Doppel SAT provides tailored content for every scenario, and the ability to custom-build content specifically for your business.

- **Built-for-you with AI Content Builder**: Create custom training courses based on company protocols in just a few clicks. We can ingest training goals, source materials like internal policies, and branding to build a fully custom training course in minutes.

- **Deepfake-Driven Customization:** Generate training videos of your own CEO or department heads delivering time-sensitive security updates.

- **Just-in-Time Reinforcement:** Users receive micro-quizzes and coaching the moment they fail a simulation, ensuring the lesson sticks.





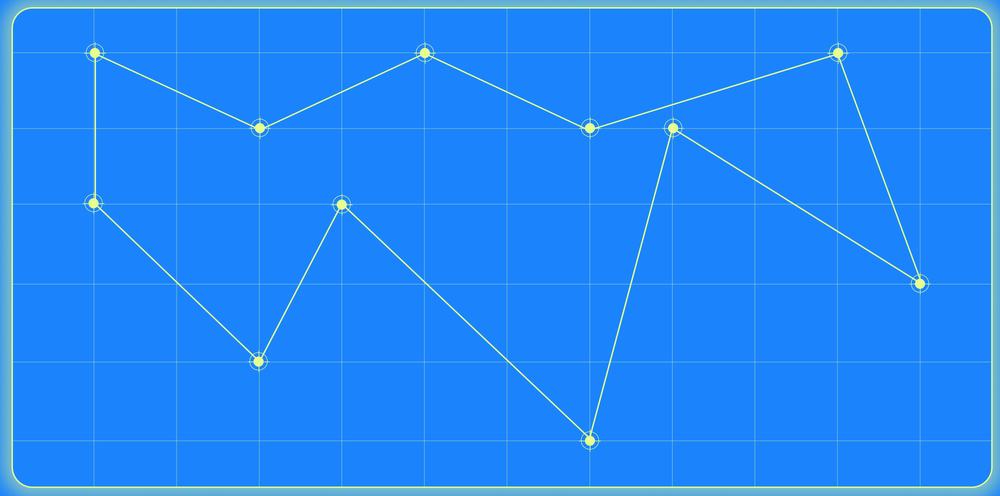
3. Risk Modeling: The Intelligence Layer

We aggregate data from every channel to identify your highest-risk users.

- **Heatmaps and Susceptibility Scoring:** Visualize which departments (e.g., finance or engineering) are failing specific types of attacks, and gain insight into user-level confidence, strengths, weaknesses, and behavior patterns
- **Leaderboards**: Reward vigilance. Instead of a punitive culture, build a culture of security champions.
- **Phishing Triage**: Create a continuous feedback loop by empowering employees to report suspicious emails and rewarding vigilance.

THE BOTTOM LINE

Doppel is the only platform that closes the loop between Digital Risk Protection (what's happening outside) and Human Risk Management (how your people respond).

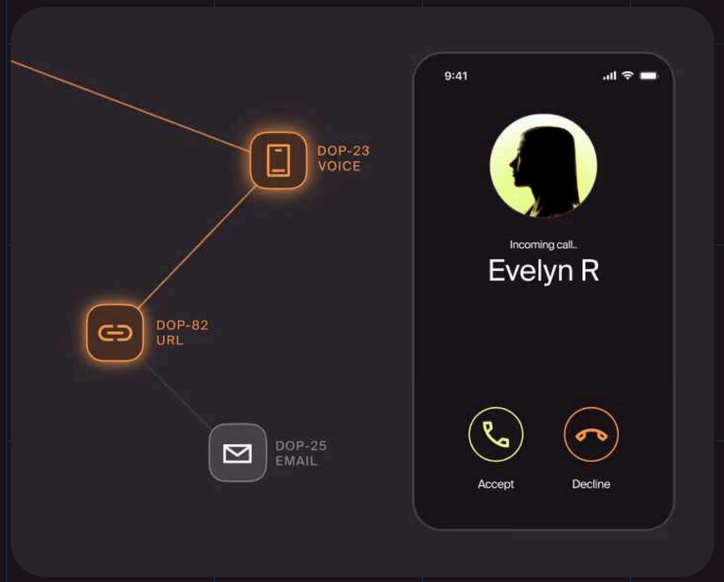


CHAPTER 4

Your Migration Framework

A Tactical Guide to Modernizing Your Defense

Consider this your quickstart roadmap for moving from a legacy SAT vendor to an AI-native HRM program.



Choose Your Entry Point

While the ultimate goal is the same (measurable behavioral change), organizations typically choose one of two paths to begin their HRM journey:

1. The "Blind Spot" Audit

Run a baseline multi-channel simulation (email + SMS) without prior announcement. Compare these results to your legacy email-only stats. This provides the most accurate raw data, but can be a shock to the system for some workforces.

2. Culture-First Alignment

Focus on transparency and buy-in. Before launching any simulations, engage with HR, legal, and department heads to explain the shift from compliance to resilience. Announce that training is moving from generic videos to active, real-world scenarios designed to protect the employees, not just catch them.

Discovery and Behavioral Baselining

3. IDP Integration

Connect Doppel to your Identity Provider (Okta, Azure AD) to map users to their roles and access levels.

4. Define High-Risk Cohorts

Identify the users who hold the keys to the kingdom (e.g., admins, execs, finance).

Deploying the Agentic Defensive

5. Launch Vibe Phishing Simulations

Use Doppel's natural language prompts to create branded, role-specific lures (e.g., "New Expense Policy for the Finance Team").

6. Helpdesk Pressure Test

Launch vishing simulations against your BPO, contact center, or internal support teams to ensure they aren't falling for urgent executive voice clones.

7. Threat-to-Sim Workflow

Activate threat cloning. If Doppel DRP detects a new phishing domain targeting your brand, it automatically pushes a simulation of that exact attack to your employees within the hour.

Behavioral Architecture and SAT 2.0

8. Deepfake Training Rollout

Replace generic Security 101 videos with a 2-minute custom deepfake video of your CISO explaining a real attack the company just blocked.

9. Automated Nudging

Enable AI-driven coaching. If a user clicks an SMS link, they are automatically given a step-by-step review of the simulation and a quiz about what they should have noticed. If they answer incorrectly, they're enrolled in a 30-second learning module on their mobile device.

10. Gamification

Launch the organizational leaderboard. Publicly reward the department with the highest reporting rate.

Optimization and Executive Reporting

11. The Risk Reduction Report

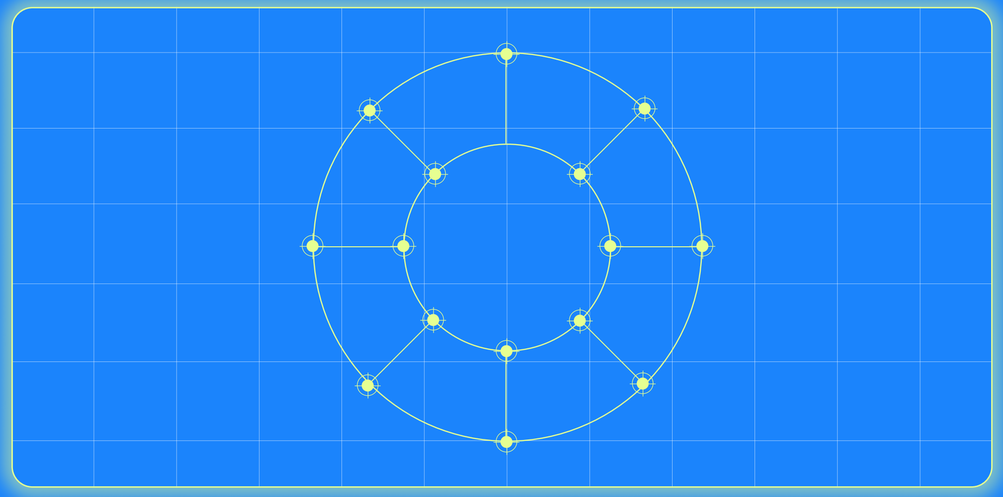
Prepare your board deck. Don't just show click rates. Show the reduction in risk velocity and how your helpdesk's success rate in identifying voice clones has improved.

12. Policy Automation

Use Doppel Risk Scores to trigger technical responses (e.g., "Users with a risk score above 80 must undergo mandatory hardware-key MFA").

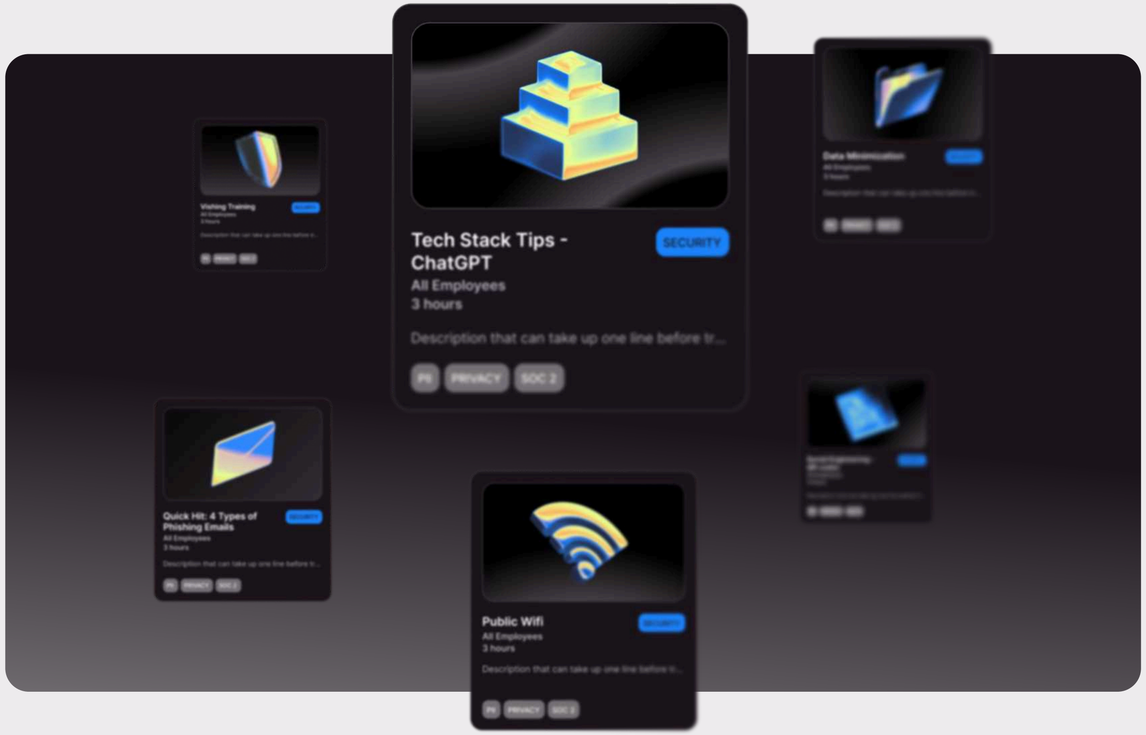
THE BOTTOM LINE

By the end of your implementation, you have moved from a "set it and forget it" training tool to an active, intelligence-driven defense system that identifies risk before it becomes a breach.



Why Legacy SAT is Your Biggest Blind Spot

Legacy vendors focus on the quantity of content. Doppel focuses on the quality of defense.



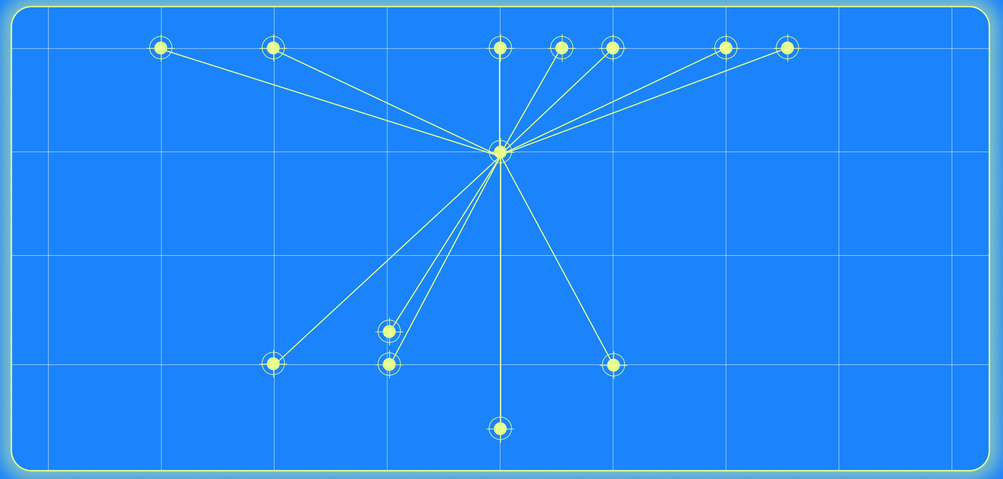
Legacy vendors focus on the quantity of content. Doppel focuses on the quality of defense.

Feature	Legacy vendors (SAT)	Doppel HRM
Channels	Email-only	Email, SMS, Voice, Telegram, Microsoft Teams, Zoom
Simulations	Static Templates	Fully Custom, Built with Agentic AI & Threat-Informed
Intelligence	Siloed	Integrated with DRP & Doppel Threat Graph
Training	Generic Video Library	Deepfake-driven & Custom GenAI content creation, and threat-informed courses
Goal	Vanity Metrics & Low Click Rate	Behavior Change & Risk Reduction

Legacy tools give you a post-breach analysis. You'll learn what happened retroactively, but you won't be able to adapt to the attacker's next move. Doppel helps you defend proactively, not after the fact.

THE BOTTOM LINE

Staying with a legacy vendor isn't just a budget choice; it's a security risk. Every day you spend on email-only simulations is a day your helpdesk remains vulnerable to a deepfake voice attack.



CASE STUDY

HRM in the Real World

In the previous chapters, we covered how legacy training is failing because it treats the inbox as the only field of battle. But as the human element is not a static target. To move from theoretical compliance to actual HRM, a security leader must ask:

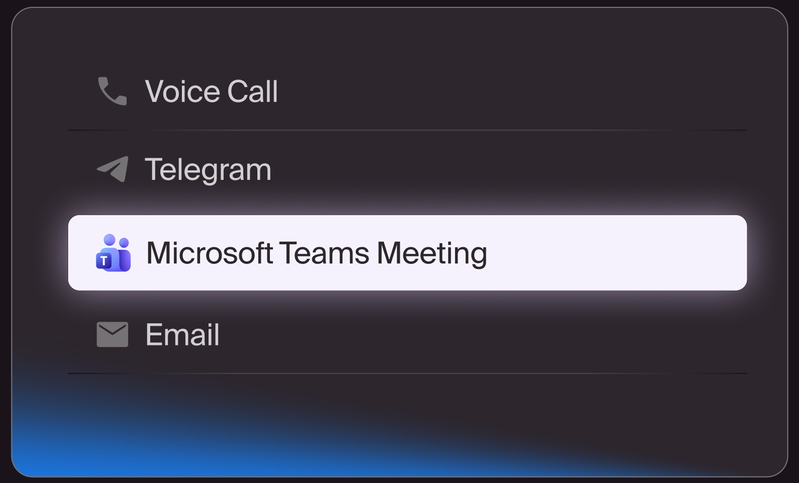
Where does my team actually live and work?

For Permiso, a leader in identity security, the answer wasn't just email. It was Microsoft Teams. They realized that while their security program had high visibility into email-based threats, they were essentially blind to the implicit trust gap inherent in collaboration tools. Permiso recognized that if they only simulated email phishing, they were optimizing for a reality that no longer existed.

PERMISO

To bridge this gap, Permiso partnered with Doppel to launch the industry's first agentic simulation within Microsoft Teams. This interactive AI agent joined native meetings to engage employees in real-time, not to test if they clicked a malicious link.

To test contextual pressure, the simulation even utilized a voice-cloned persona of Permiso's Co-CEO, Jason Martin. The simulation meant the difference between checking a box and actually hardening the perimeter:



> "Doppel fundamentally changed how we think about human risk. It's not just about running better simulations; it's about testing how attacks actually happen across channels. The Microsoft Teams simulation campaign showed us where our real exposure was, and gave us a way to measure and improve it. That's the difference between a program that looks good on paper and one that actually reduces risk."

Jason Martin
Co-CEO and Co-Founder,
Permiso

CONCLUSION

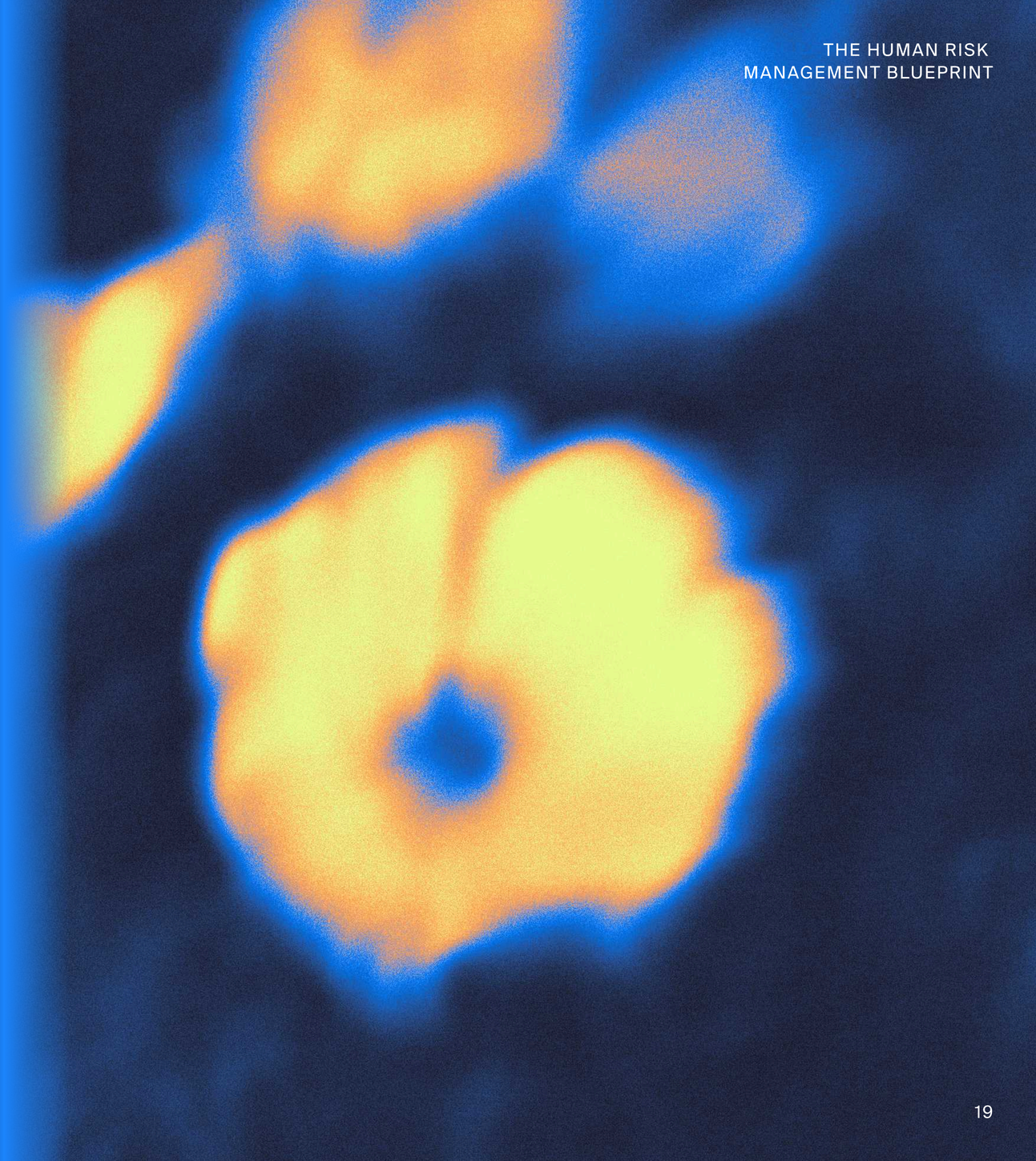
The Future is Resilient

Your workforce isn’t your greatest weakness.

When armed with agentic simulations, threat-informed training, and dynamic risk scoring, your employees become your strongest perimeter.

The shift from SAT to HRM is the most important move a security leader can make in 2026. This blueprint is your starting line.

The attackers have already automated. Now, it's your turn.



Doppel

Learn more about Doppel, and take a guided demo to see what we discussed here in action.

Book a 1:1 demo with an HRM expert to map your migration from legacy training to an active, agentic defense.

Book a demo

©2026 DOPPEL INC.