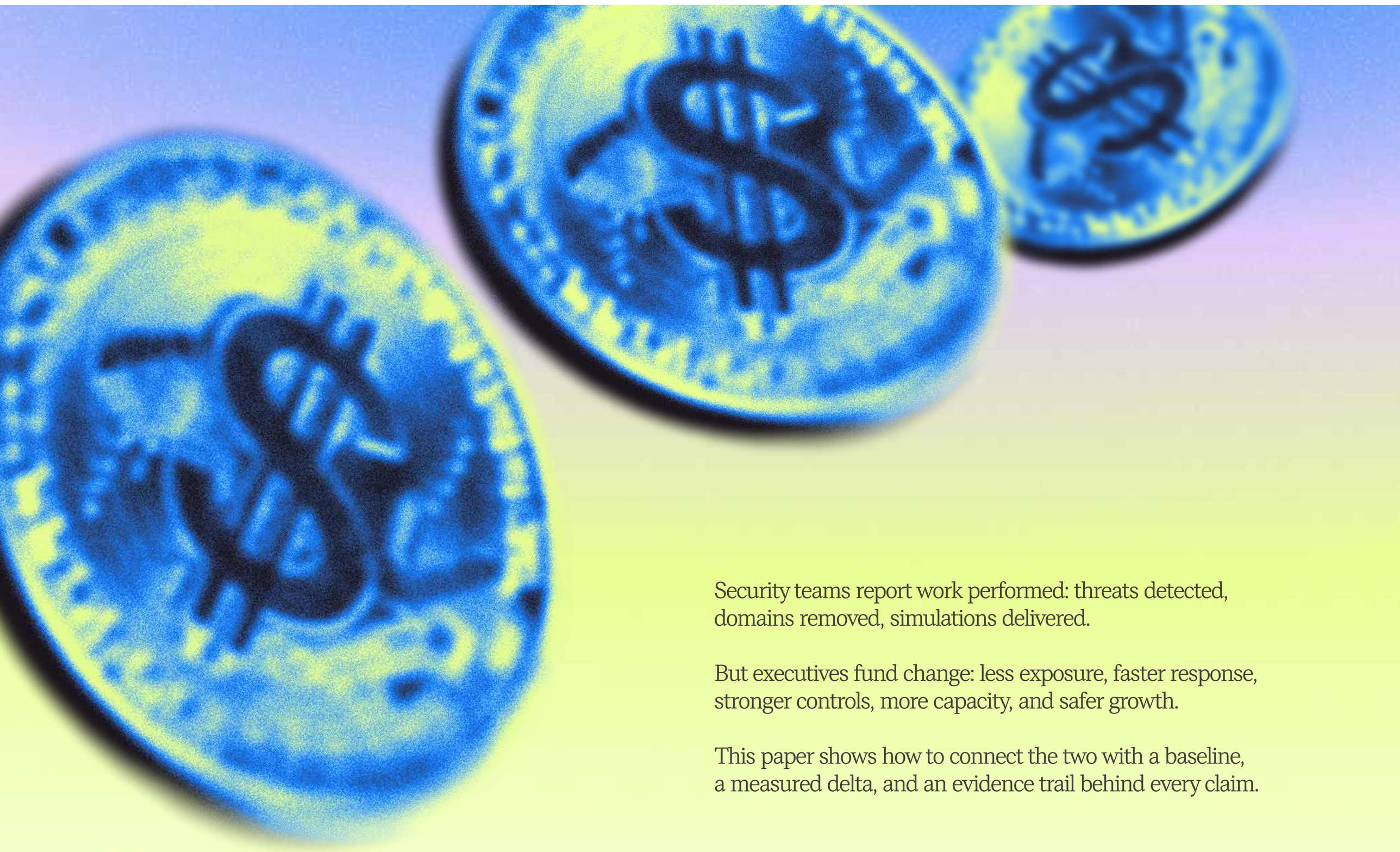
©2026 DOPPEL INC.

The Business Value of Social Engineering Defense

Measure social engineering defense by the business outcomes it creates, not the security activity it produces.



Security teams report work performed: threats detected, domains removed, simulations delivered.

But executives fund change: less exposure, faster response, stronger controls, more capacity, and safer growth.

This paper shows how to connect the two with a baseline, a measured delta, and an evidence trail behind every claim.

© Doppel Inc. 2026. All Rights Reserved.

Doppel

Close the security value translation gap

Security teams typically roll up key metrics to show the work a program delivers:

- Threats detected
- Alerts triaged
- Domains removed
- Simulations delivered
- Employees trained

These are meaningful operating measures.

Executives ask different questions:

Is financial exposure shrinking?

Are customers seeing fewer impersonations?

Could our help desk withstand a convincing impersonation of one of our executives?

The distance between those two conversations is the security value translation gap.

It is where many programs lose budget arguments, not because the work lacks value, but because the report does not show it.

The board and C-suite think in terms of revenue, risk, and reputation. A security update built on tactical counts leaves them to guess at the business value.[1]

Social engineering widens the gap. These attacks exploit trust: customers trusting a brand, employees trusting an executive, help desks trusting an identity claim. A single campaign often links a fraudulent domain, a convincing message, and a manipulated business process.

Counting the pieces shows how busy the defense is. It does not show whether the attacker's window is closing.

Activity metrics remain useful as operating measures. Their business meaning depends on context. A takedown matters when it shortens the time an attacker has to reach customers. A simulation matters when it exposes a weakness in help desk verification and leads to stronger adherence to the process.

The value of social engineering defense lives in the change it creates. Measure the baseline, measure the delta, and connect both to the business outcome they serve.

The value of social engineering defense lives in the change it creates.

Measure the baseline, measure the delta,
and connect both to the business outcome they serve.

[1] Ines Marjanovic, "How to Report Brand Risk to the Board: Translating Security into Revenue," Doppel blog, https://www.doppel.com/blog/report-brand-risk-board

© Doppel Inc. 2026. All Rights Reserved.

Doppel

From activity to value

Value doesn't come down to one number. It's a chain of claims, and each claim needs its own evidence. The value translation ladder shows how a security activity climbs to a business result.

LAYER	EXAMPLE	EVIDENCE REQUIRED
Security activity	Malicious domains removed	Takedown records and ticket history
Security outcome	Attacker infrastructure taken offline	Verification that the asset is no longer live
Risk reduction	Malicious assets stay active for less time	Active duration before and after, for comparable threats
Business outcome	Fewer customers exposed to impersonation	Reported impersonations, scam-related contacts, recurrence
Business value	Lower fraud exposure and scam-related support effort	Loss data, support cost, and a supported attribution

When you build a value case, trace each claim up the ladder. Removing a malicious domain supports an infrastructure claim. Connecting that removal to financial benefit takes information about exposure, potential loss, and attribution. If the evidence stops at the first rung, the claim should stop there too.

© Doppel Inc. 2026. All Rights Reserved.

Doppel

Five outcomes executives fund

The same five outcomes organize the value of social engineering defense. Each pairs an executive question with an external contribution, a human contribution, and representative proof. External defense reduces the attacker's ability to establish, operate, and scale malicious infrastructure. Human defense strengthens the people and processes attackers try to manipulate.

OUTCOME	EXECUTIVE QUESTION	EXTERNAL DEFENSE	HUMAN DEFENSE	REPRESENTATIVE PROOF
Protect revenue	Where can money be lost?	Shorter exposure windows	Hardened payment, account, and helpdesk workflows	Exposure duration; workflow readiness
Preserve trust	Do customers trust what they see?	Fewer brand and executive impersonations	Faster reporting and escalation	Recurrence; scam-related contacts
Reduce risk	Is the organization more resilient?	Correlated campaigns; documented mitigation	Measured improvement in vulnerable cohorts	Repeat failures; post-intervention improvement
Improve efficiency	Are we protecting more with the same effort?	Automated triage and enforcement	Automated campaigns and reporting	Handling time; manual handoffs
Enable secure growth	Can protection keep pace with the business?	Coverage for new brands and markets	Testing for new channels and populations	Onboarding time; coverage gaps closed

The sections on the following page show each outcome in practice, with a real-world organization that made it a priority.

© Doppel Inc. 2026. All Rights Reserved.

Doppel

Protect revenue

Money is lost where trust is exploited: a fraudulent checkout page, a spoofed invoice, a manipulated account change. Protecting revenue means shrinking the time and the places an attacker can operate. Measure exposure duration, unresolved threats, and the readiness of revenue-critical workflows.

ADVANCE[2]

WHAT MATTERS MOST

Shrinking the window attackers have to reach customers.

BASELINE

Domain takedowns averaged 30 days, and the team completed roughly 10 successful takedowns a year.

DELTA

Takedown timelines dropped to under one week. Successful takedowns grew to more than 150 in the first year and 250 in the second.

WHAT IT LEADS TO

Faster response and greater throughput lead to a shorter window for attackers to reach customers and fewer opportunities for fraud and customer diversion.

Preserve trust

Trust is the asset attackers borrow. Every convincing fake carries the credibility of the real brand. Measure whether customers and stakeholders encounter less confusion: impersonation recurrence, scam-related contacts, and response speed.

ARK INVEST[3]

WHAT MATTERS MOST

Keeping customers from encountering impersonations and scams that borrow ARK's name.

BASELINE

Scam takedowns took weeks, and ARK received approximately 400 reports of impersonations and scams in 2024.

DELTA

Median domain resolution time is 5.5 hours, takedown success is 98%, and reported impersonations and scams fell to roughly half that number in 2025.

WHAT IT LEADS TO

Fewer impersonations in circulation means fewer moments where a customer's confidence in ARK is at risk, which protects trust in the brand and its interactions with customers.

ARK's CTO describes the results as "a new benchmark in the realm of online brand protection."[4]

[2]Doppel, "Advance Dismantles Social Engineering Campaigns at the Source," customer story, accessed Oct. 21, 2026, https://www.doppel.com/customers/advance.
[3]Doppel, "From Weeks to Minutes: Why ARK Invest Chose Doppel to Automate Social Engineering Defense," customer story, accessed Oct. 21, 2026, https://www.doppel.com/customers/ark-invest.
[4]Mark Keller, CTO, ARK Invest, in Doppel, "Customers Love Doppel," accessed Oct. 21, 2026, https://www.doppel.com/customer-love.

© Doppel Inc. 2026. All Rights Reserved.

Reduce risk

Risk falls when the probability or the impact of a successful manipulation falls. Combine external exposure measures with human and process evidence: repeat failures, reporting speed, verification adherence, and improvement after intervention.

PERMISO[5]

WHAT MATTERS MOST

Finding where employees are actually vulnerable, in the channels attackers use.

BASELINE

Permiso's human risk program centered on email-based simulations.

DELTA

Permiso, an identity security company, expanded its program beyond email and became the first organization in its industry to run a phishing simulation through a Microsoft Teams meeting. In realistic, conversational scenarios, an AI agent took on the voice and persona of its Co-Founder and Co-CEO to test how employees respond to executive pressure.

WHAT IT LEADS TO

The campaign surfaced exposure that email-based simulations had not, which leads to a more accurate foundation for measuring and reducing human risk.

Permiso's co-CEO describes the approach as "testing how attacks actually happen across channels."[6]

Improve efficiency

Attack volume grows faster than headcount. Efficiency means protecting more with the same effort. Measure handling time, manual handoffs, and backlog. Treat hours released as operating capacity. They become cost savings only when spending changes.

REA Group[7]

WHAT MATTERS MOST

Taking manual effort out of takedowns so the team can protect the brand at scale.

BASELINE

REA Group operates Australia's leading property websites, and its team was finding impersonation campaigns that its previous brand protection tool had not detected.

DELTA

In a two-week proof of concept, Doppel found more fake apps than REA had identified in the previous year. REA now automates high-confidence takedowns across its portfolio, triggered by tickets from its customer-facing fraud team.

WHAT IT LEADS TO

Automation shifts the team away from manual takedown tasks, which means it can cover more with the same effort.

REA's head of cyber defence says automation has "removed a huge amount of manual work."

[5]Doppel, "How Permiso Is Securing the Modern Attack Surface with Doppel," customer story, accessed Oct. 21, 2026, https://www.doppel.com/customers/how-permiso-securing-modern-attack-surface-doppel.
[6]Jason Martin, Co-CEO and Co-Founder, Permiso, in Doppel, "Customers Love Doppel," accessed Oct. 21, 2026, https://www.doppel.com/customer-love.
[7]Doppel, "REA Group Protects Its Brands and Reputation with Social Engineering Defense," customer story, accessed Oct. 21, 2026, https://www.doppel.com/customers/rea-group-protects-its-brands-and-reputation-social-engineering-defense.

© Doppel Inc. 2026. All Rights Reserved.

Enable secure growth

Growth adds brands, markets, channels, and workflows, and each one adds attack surface. Secure growth means protection extends as fast as the business does. Measure onboarding time for new brands, coverage gaps closed, critical workflows tested, and the effort required to sustain coverage.

APTOS[8]

WHAT MATTERS MOST

Extending protection beyond external threats to employees, within one program.

BASELINE

The Aptos Foundation supports an ecosystem of more than 330 projects, and that visibility makes it a target for sophisticated social engineering. It was already using Doppel Digital Risk Protection (DRP) to take down fake domains, impersonators on X, and malicious Telegram bots, coverage its previous services did not provide on those channels.

DELTA

The Foundation added Doppel Human Risk Management (HRM), so employees now train against realistic, multi-channel simulations across email, SMS, and other channels, built with real-world threat intelligence. External takedowns are complete in less than three days, and both defenses now run in one program that covers the full attack lifecycle.

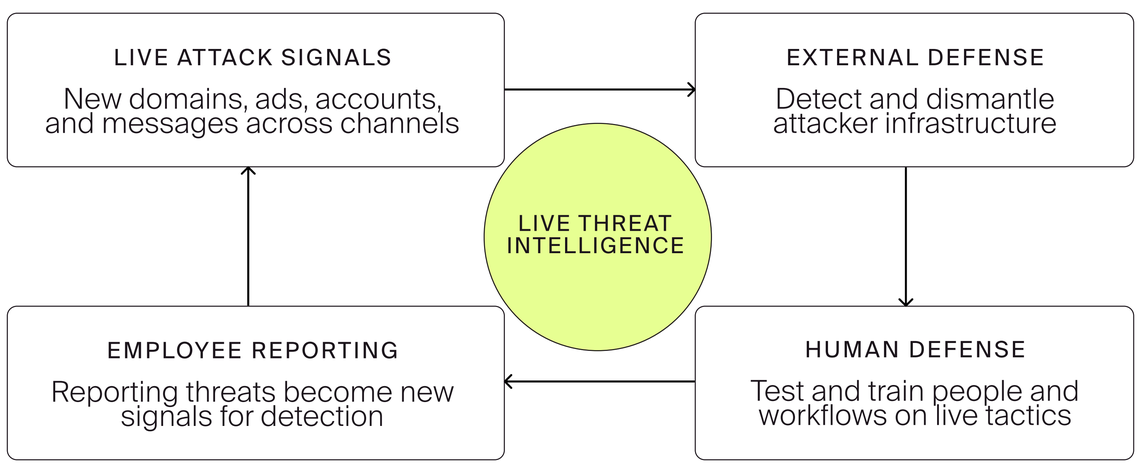
WHAT IT LEADS TO

Covering both the attacker's infrastructure and the employee's decision in one program lets protection keep pace with a growing ecosystem without slowing the workforce.

Why connected defense compounds

Every social engineering attack has two parts: infrastructure and a human decision. A fraudulent domain gives an attacker somewhere to operate. An impersonated executive gives a request credibility. A conversation creates pressure to act. Defending only one part leaves the other exposed.

At Doppel, we don't think infrastructure and people should be defended separately, which is why we built Social Engineering Defense (SED) as one connected program.



When the two sides share intelligence, each improves the other. External attack patterns inform realistic simulations and targeted training. Threats that employees report strengthen detection and response outside the organization.

The connection also makes value easier to show. Track three things:

01 How quickly a detected threat becomes a relevant test

02 Whether verification behavior improves after targeted training

03 Whether employee reporting speeds up intervention

> The Aptos Foundation story above shows the model in practice: one program covering both the attacker's infrastructure and the employee's decision.

[8]Doppel, "How the Aptos Foundation Secures the Future of Web3 with Doppel's Social Engineering Defense," customer story, accessed Oct. 29, 2026, https://www.doppel.com/customers/aptos-foundation

© Doppel Inc. 2026. All Rights Reserved.

Give every value claim an evidence trail

Security leaders earn executive trust when every number they present says how certain it is. Doppel's business value approach helps you do that: we establish a baseline, track what changes after each intervention, and sort every result into one of three types, so the outcomes you drive hold up in the boardroom.

CLAIM TYPE

Observed

DEFINITION

Directly measured

EXAMPLE FROM THIS DOPPEL CUSTOMERS

ARK Invest's 5.5-hour median domain resolution time

Advance's move from 30-day takedowns to under one week

CLAIM TYPE

Influenced

DEFINITION

Supported by evidence but affected by other variables

EXAMPLE FROM THIS DOPPEL CUSTOMERS

ARK Invest's decline in reported impersonations and scams

CLAIM TYPE

Modeled

DEFINITION

Estimated using explicit, agreed assumptions

EXAMPLE FROM THIS DOPPEL CUSTOMERS

Estimated fraud loss avoided, based on customer-specific loss assumptions

Dollar figures belong at the modeled end of this scale until losses or spending have been documented as lower.

When your CFO asks for one, three calculations cover most questions:

LAYER	EXAMPLE	EVIDENCE REQUIRED
Capacity value	Validated hours released × customer-loaded hourly cost	Hours released are capacity, not cash savings
Modeled risk reduction	Change in event likelihood × customer-relevant financial impact × supported attribution	An estimate; label it as modeled
Realized financial benefit	Documented reductions in losses or spending	Requires records, not assumptions

Doppel's business value team works with security leaders to build this trail: establishing the baseline, agreeing on success measures and assumptions, validating what changed, and tying each result to the outcome your executives care about.

© Doppel Inc. 2026. All Rights Reserved.

FOUR RULES KEEP YOUR NUMBERS DEFENSIBLE:

01 Report observed results and modeled estimates separately.

02 Count overlapping contributions from external and human defense once.

03 Compare equivalent periods, channels, and populations, and record changes in attack volume and simulation difficulty.

04 Retain the source, period, owner, and assumptions behind every claim.

The goal is a claim that survives scrutiny when your CFO asks a follow-up question. That's how security leaders turn the outcomes they drive with Doppel into value the business recognizes.

Make the change visible

When you report results, build the executive readout around three questions:

QUESTION 01

What changed?

Name the baseline and the delta.

QUESTION 02

What evidence supports it?

Classify each claim as observed, influenced, or modeled.

QUESTION 03

Why does it matter to the business?

Tie the change to one of the five outcomes.

You don't need a new platform to begin. You need a baseline. Capture these five measures before any change, then revisit the same measures after each intervention.

BASELINE MEASURE	WHAT TO CAPTURE	OUTCOME IT INFORMS
Threat duration	How long malicious domains, accounts, and ads stay active, from detection to resolution	Protect revenue Preserve trust
Response time	Time to detect, escalate, and resolve; time for employees to report a suspicious message	Reduce risk
Manual effort	Handling time, manual steps, handoffs, and backlog	Improve efficiency
Tested behaviors	How employees respond in realistic, multi-channel tests, including payment and help desk workflows	Reduce risk Protect revenue
Coverage	Brands, executives, channels, and employee populations protected or tested, and where coverage ends	Enable secure growth

© Doppel Inc. 2026. All Rights Reserved.

Next step:

Start with a baseline workshop. In one session, a security team and its business stakeholders can map current activity to the five outcomes, identify the evidence already available, and agree on the measures to track.

SCHEDULE A BASELINE WORKSHOP

How Doppel helps

Doppel is the AI-native platform for Social Engineering Defense (SED), built to defend across the social engineering attack chain. It protects people and brands from AI-powered impersonation, phishing, fraud, and deception through three solutions:

DIGITAL RISK PROTECTION (DRP)

sees attacks forming and dismantles attacker infrastructure.

HUMAN RISK MANAGEMENT (HRM)

Hardens the people attackers target.

EMAIL SECURITY

Defends the inbox where deception lands.

Every signal flows through a shared Doppel Threat Graph, so a threat seen anywhere strengthens defenses everywhere. Campaigns are eliminated at the source, and every takedown raises the attacker's cost.

Doppel customers use this kind of baseline to show what changed across external threats and human behavior.

Or learn more about the Doppel platform.

Request a demo to see how Doppel SED can help you do the same.

REQUEST A DEMO

© Doppel Inc. 2026. All Rights Reserved.