outtake labs

2026 Digital Trust Industry Pain Report

The Internet Is No Longer A Human Space.

And most security programs don't know it yet.
Agentic AI has flooded the open internet with non-human infrastructure at a scale that dwarfs anything humans have built. Adversaries understood this shift first. They weaponized it. Against your brand. Your executives. Your customers' trust. What follows is the data that proves it.

01

The Rules Have Changed

Trust is the primary target now, not infrastructure.

02

The Treat Has Automated

Speed and scale no human team was built to match.

03

Every Industry. Same Pattern.

In organizations that look like yours. Right now.

NAVIGATION

Table of Contents

SECTION 01

Executive Summary

One Report. One Alarming Pattern.

This report presents the first cross-industry mapping of digital trust failures, based on analysis of 75 organizations across more than 20 sectors. Our research combines frontline security intelligence, insights from CISO-level conversations, and validated incident data, all mapped against a newly developed framework: the Digital Trust Kill Chain.

Every Industry. All Losing Ground.

The findings are clear: organizations are losing ground. The attack surface is expanding faster than defenders can manage, while AI-driven threat automation has outpaced traditional detection tools. At the same time, trust identity: brand, executive presence, and domain credibility, has become the primary target for modern adversaries.

Real Incidents. Real Losses. Real Risk.

This is not a theoretical landscape. Every insight in this report is grounded in real-world incidents and actual losses. The voices represented, from CISOs to security architects and fraud operations leaders, reflect what is actively breaking down in today's environments.

SECTION 01

Executive Summary

75 ORGANIZATIONS ANALYZED	20+ INDUSTRY VERTICALS MAPPED
6 DOMINANT PAIN CATEGORIES IDENTIFIED	12/20 VERTICALS HIT BY EXECUTIVE IMPERSONATION

KEY FINDING

Organizations are not losing ground because they can't detect threats. They're losing ground because they can't prioritize and respond to them fast enough. Alert fatigue, manual workflows, and fragmented tooling are giving AI-powered attackers a decisive and growing advantage. Across every industry analyzed, this was the single most consistent failure point.

The attack has already automated. The defense hasn't.

SECTION 01

Executive Summary

01

Brand Impersonation At Industrial Scale

Fake domains, social media accounts, and executive impersonations are being deployed in coordinated campaigns, not isolated incidents. Some organizations face hundreds of concurrent scam assets at peak.

02

AI-Accelerated Attack Volume

AI is enabling attackers to generate, deploy, and rotate malicious infrastructure, including domains, fake accounts, and synthetic personas, at a pace that overwhelms traditional detection and manual review processes.

03

Expanding Platform Blind Spots

Channels such as Telegram, WhatsApp, TikTok Shop, and emerging AI agents introduce visibility gaps. Security teams often lack coverage in these environments, allowing threats to operate undetected until significant damage has occurred.

SECTION 02

The Agentic AI Threat Backdrop

To understand the 2026 digital trust landscape, you must first understand the force multiplier that has rewritten the rules of engagement: agentic AI operating at internet scale.

The Core Problem

Bots, especially AI-driven ones, now dominate web traffic, making the identification of real users and malicious actors exponentially more difficult. Threat automation is scaling faster than defenses, reducing the effectiveness of legacy security tools. AI accelerates both attack sophistication and volume simultaneously, necessitating adaptive defenses that detect patterns rather than rely on static rules.

Automation Outpaces Defense

Adversaries are deploying AI to run automated reconnaissance, generate convincing phishing content, spin up fake infrastructure, and rotate attack vectors, all in continuous, adaptive loops that legacy rule-based tools were never designed to counter.

Bot Traffic Dominates The Web

A growing share of all internet traffic is non-human. Security teams are effectively trying to find malicious signals in an ocean of automated noise. Real user behavior and bot behavior are increasingly indistinguishable without AI-native detection.

Adaptive Vs. Static

Static signature rules and blacklists are insufficient. The 2026 threat environment demands real-time pattern recognition across diverse signals: domain registration behavior, social account growth patterns, and campaign coordination. Not post-hoc incident matching.

SECTION 03 — INDUSTRY FIRST

The Digital Trust Kill Chain

Outtake Research Labs has developed the industry's first Digital Trust Kill Chain, an 8-stage framework mapping how adversaries systematically dismantle organizational trust, from initial reconnaissance to final monetization. Each stage includes observed attack technique prevalence drawn from our 75-organization dataset.

Traditional kill chains model network intrusion. The Digital Trust Kill Chain models something different and more insidious: the systematic exploitation of brand identity, executive credibility, and institutional reputation as attack vectors. Understanding which stage you're being targeted at determines your entire response strategy.

Zone 1 · OSINT	Zone 1+2	Zone 2 · Threat	Zone 3 · DRP	Zone 3+4	Zone 4 · Fusion	Zone 4 · Fusion	Zone 4 · Fusion
01	02	03	04	05	06	07	08
Reconnaissance	**Infrastructure Setup**	**Trust Exploitation**	**Target Engagement**	**Credential Capture**	**Account Takeover**	**Impact & Fraud**	**Monetization**
Gathering intel on targets	Building attack resources	Abusing brand and identity	Contacting victims	Stealing authentication	Gaining unauthorized access	Executing the scam	Converting to profit

01 Agentic OSINT — Early Detection

Detects reconnaissance targeting brand, executives, and partners. Identifies fake infrastructure: domains, apps, accounts, ads, as it's created. Exposes trust exploitation before campaigns launch.

✓ Disrupts: Reconnaissance · Infrastructure Setup · Trust Exploitation

02 Threat Graph — Pattern Recognition

Maps relationships between fake accounts, domains, ads, and narratives. Identifies coordinated campaigns and adversarial networks, including the Telegram/WhatsApp terminal pivot documented across 8+ accounts.

✓ Disrupts: All stages — links dispersed threats into actionable intelligence

03 Agentic DRP — Automated Disruption

Removes fake domains, apps, social accounts, and malicious ads. Dismantles phishing and credential capture infrastructure. Takes down entire adversarial networks, not just individual threats.

✓ Disrupts: Infrastructure · Engagement · Credential Capture · Account Takeover

04 Cyber Fraud Fusion — Predictive Defense

Correlates external OSINT with internal fraud signals to predict emerging attacks. Proactively blocks threats: wire fraud, direct payout, IP abuse, exec safety, before they reach customers or cause business impact.

✓ Disrupts: All stages, through predictive intelligence and automated prevention

SECTION 04

Industry Pain Map

The following table synthesizes primary pain categories observed across all verticals analyzed. Pain categories are ranked by prevalence within each vertical. * denotes an emerging or particularly acute signal.

Pain Category Definitions: CRED PHISH = Credential phishing attacks targeting users or employees. **PAYOUT** = Direct financial fraud or scam-driven cash transfers. **BRAND/REP** = Brand impersonation or reputation damage campaigns. **EXEC SAFETY** = Executive impersonation and/or physical safety threats. **REC. FRAUD** = Recruiting fraud using fake job postings or personas. **IP/COUNTER**. = Intellectual property theft or counterfeit goods.

VERTICAL	PRIMARY PAIN	SECONDARY PAIN
Private Equity & Investment Managers	CRED PHISH	PAYOUT
Hedge Funds	PAYOUT	BRAND/REP
Retail Banks & consumer Fintech	CRED PHISH	PAYOUT
Insurance	EXEC SAFETY	CRED PHISH
Defense & Aerospace	REC. FRAUD	EXEC SAFETY
Enterprise SaaS, Dev Tools & Cloud	CRED PHISH	REC. FRAUD
AI Labs	CRED PHISH	EXEC SAFETY
Large Tech / Platform	CRED PHISH	EXEC SAFETY
Luxury Goods	PAYOUT	IP/COUNTER
Consumer & Mass Retail	IP/COUNTER	CRED PHISH
Food, Beverage & CPG	BRAND/REP	IP/COUNTER
Healthcare & Medtech	EXEC SAFETY	CRED PHISH
Mining, Energy & Resources	PAYOUT	CRED PHISH
Consulting & Professional Services	BRAND/REP	EXEC SAFETY
Talent Agencies & Celebrity Mgmt	PAYOUT	BRAND/REP
Individual Creators & Wellness	PAYOUT	IP/COUNTER
Media & Broadcasters	PAYOUT	IP/COUNTER
Live Events, Sports & Streaming	IP/COUNTER	BRAND/REP
Government & Nonprofit	IP/COUNTER	CRED PHISH
Airlines & Aviation	CRED PHISH	BRAND/REP

SECTION 05

Financial Services

Financial services firms face a convergence of the highest-value targets and the most sophisticated adversary toolkits. Wire fraud, LP distribution intercepts, and executive impersonation-driven investment scams represent existential reputational and financial risks that dwarf most other verticals.

Private Equity & Investment Managers

BRAND/REP

PAYOUT

Hedge Funds

BRAND/REP

PAYOUT

Retail Banks & Consumer Fintech

PAYOUT

SECTION 06

Enterprise Technology & AI

Technology companies occupy a uniquely exposed position: they are simultaneously high-value targets due to their data and infrastructure, and their own tools — developer platforms, cloud APIs, AI systems — are being weaponized against them. The blind spots are widening faster than security teams can instrument.

AI Labs

CRED. THEFT

EXEC SAFETY

PAYOUT

Large Tech / Platform Companies

CRED. THEFT

EXEC SAFETY

BRAND/REP

Enterprise SaaS, Dev Tools & Cloud

CRED. THEFT

REC. FRAUD

BRAND/REP

Defense & Aerospace

REC. FRAUD

EXEC SAFETY

Consulting & Professional Services

BRAND/REP

EXEC SAFETY

SECTION 07

Consumer, Retail & Brand Industries

Consumer-facing brands operate at the intersection of massive public visibility and distributed attack surfaces. Their reputations are their most valuable asset, and the most easily weaponized by adversaries running counterfeit, impersonation, and crisis-exploitation campaigns at scale.

Luxury Goods

PAYOUT

IP/COUNTER

Consumer & Mass Retail

IP/COUNTER

REC. FRAUD

BRAND/REP

Food, Beverage & CPG

BRAND/REP

IP/COUNTER

REC. FRAUD

Talent Agencies & Celebrity Management

PAYOUT

BRAND/REP

IP/COUNTER

EXEC SAFETY

Individual Creators & Wellness

PAYOUT

IP/COUNTER

Live Events, Sports & Streaming

IP/COUNTER

BRAND/REP

EXEC SAFETY

SECTION 08

Healthcare, Government & Other Verticals

Healthcare and government entities represent some of the most consequential targets in the dataset — not just for financial fraud, but for attacks that translate directly into physical harm and public safety consequences. The stakes could not be higher.

Healthcare & Medtech

EXEC SAFETY

IP/COUNTER

Government & Nonprofit

PAYOUT

IP/COUNTER

Insurance

EXEC SAFETY

BRAND/REP

Mining, Energy & Resources

PAYOUT

REC. FRAUD

EXEC SAFETY

Airlines & Aviation

BRAND/REP

Media Companies & Broadcasters

PAYOUT

IP/COUNTER

EXEC SAFETY

BRAND/REP

SECTION 09

Cross-Cutting Themes & Strategic Implications

Across all 75 organizations and 20+ verticals, six structural themes emerge that transcend any single industry. These are the systemic failure points that define the 2026 digital trust crisis.

01 The Response Speed Gap

The most consistent finding across all verticals is not that organizations can't detect threats. It's that they can't respond to them fast enough. Alert queues overflow. Manual triage processes collapse under volume. By the time action is taken, the campaign has already run. Speed of response is the defining gap across every vertical in this dataset.

02 The Platform Blind Spot Crisis

Telegram, WhatsApp, Bluesky, TikTok, and AI agent platforms are confirmed dead zones for most security tooling. Every major vendor in this space has meaningful coverage gaps on at least one high-risk platform. The surface area is expanding faster than detection capabilities. Organizations are not losing because attacks are too sophisticated. They're losing because they literally cannot see the battlefield.

03 Executives as Attack Surface

Executive impersonation is no longer a niche threat vector. It appears as a primary or secondary pain in 12 of 20 verticals analyzed. Following high-profile incidents of executive-targeted physical violence in 2024, the threat has expanded from reputational into physical safety. Healthcare, insurance, and financial services security teams are now building integrated digital-physical protection programs for their senior leadership.

04 The Telegram/WhatsApp Terminal Pivot

One of the most consistent and underreported patterns in this dataset is the adversarial pivot from public social platforms to encrypted messaging apps as the terminal engagement layer. Initial scam exposure happens on Facebook, Instagram, or X. The actual financial fraud is consummated on WhatsApp or Telegram, outside the view of any current security tooling.

05 Data Quality as a Security Problem

Multiple verticals in this dataset are underdocumented: pain fields that don't match actual use cases, inputs without validated summaries, miscategorized threat patterns. This is not just a reporting problem. Inaccurate pain data leads to wrong security tooling decisions, misaligned vendor deployments, and unaddressed gaps. Ground truth matters.

06 Crisis as Accelerant

Across the dataset, several of the most decisive responses to digital trust threats were crisis-driven. A product liability crisis at a consumer brand, an executive safety incident at a healthcare organization, and a real-time CEO impersonation event at a resources company each compressed buying timelines dramatically and exposed a consistent pattern: most organizations have no pre-existing capability to respond. The gap is not discovered during planning. It is discovered at the worst possible moment, under active threat. Crisis removes all ambiguity about priority. The organizations that act before a crisis are the exception.

Strategic Implication For CISOs:

The 2026 threat landscape demands a fundamental shift from perimeter-and-endpoint thinking to identity-and-trust infrastructure thinking. The attack vectors in this report: brand impersonation, executive spoofing, fake domains, social engineering via encrypted channels. These do not touch the traditional security stack. They operate in the space between your firewall and your customers' trust. Defending that space requires purpose-built, AI-native tooling and a new mental model of what "the perimeter" actually means.

The Attack Has Already Automated. The Defense Has To Match It.

SECTION 10

Methodology & About Outtake Research Labs

Data Foundation:
This report is based on frontline security intelligence gathered across 75 organizations spanning 20+ industry verticals. Data sources include CISO-level interviews and validated security assessments, internal incident documentation, observed adversary campaign data, and proprietary threat signal aggregation from Outtake's agentic monitoring fleet. All organizational references in this report are reproduced from validated, anonymized summaries. Specific dollar figures referenced in findings represent documented incident losses or publicly reported values unless otherwise noted.

A Note on Statistics

All figures in this report describe the scope and findings of the Outtake Research Labs dataset. They reflect observed patterns across 75 organizations and should not be interpreted as industry-wide averages. A data-rich follow-up edition with anonymized platform statistics across a broader dataset is planned for later in 2026.

About Outtake Research Labs

Outtake Research Labs is the research division of Outtake Inc., dedicated to advancing digital trust through industry-first research. We produce independent, practitioner-grade intelligence on the evolving digital threat landscape — designed to be immediately actionable by security leaders, fraud operations teams, and risk executives.

Annual Report Commitment

The 2026 Digital Trust Industry Pain Report is the inaugural edition of what will become an annual research publication. Each year, we will expand the dataset, deepen vertical coverage, and track the evolution of the Digital Trust Kill Chain as the threat landscape changes. This report establishes the baseline.

Data Integrity Notes

Where data gaps, miscategorizations, or underdocumented accounts exist in the underlying dataset, we have flagged them explicitly rather than paper over them. Intellectual honesty about data quality is a core principle of Outtake Research Labs. Findings with thin validation are marked accordingly.

WHAT TO DO NEXT

The Data Has Spoken. Now It's Time To Act.

Across every vertical analyzed, the organizations losing ground share the same gaps. Here's where to start.

Get Full Visibility

Your brand, executives, domains, and social presence. If you can't see what's being weaponized against you, you can't stop it.

Know Your Threat Profile

Every organization's exposure is different. The mix of pain categories hitting your vertical demands a response built for your specific risk.

Stop Responding Manually

The volume of AI-powered attacks cannot be matched by human workflows. Automated detection, triage, and takedown is no longer optional.

Strategic Implication For CISOs:

The 2026 Threat Landscape Demands A Fundamental Shift From Perimeter-And-Endpoint Thinking To Identity-And-Trust Infrastructure Thinking. The Attack Vectors In This Report: Brand Impersonation, Executive Spoofing, Fake Domains, Social Engineering Via Encrypted Channels. These Do Not Touch The Traditional Security Stack. They Operate In The Space Between Your Firewall And Your Customers' Trust. Defending That Space Requires Purpose-Built, AI-Native Tooling.

The Attack Has Already Automated. The Defense Has To Match It.

See how Outtake protects organizations like yours — across every platform, every vertical, in real time.

Book A Demo

APPENDIX

Pain Category Definitions

Six primary pain categories are used throughout this report to classify the dominant threat type observed for each organization and vertical. Each category represents a distinct adversarial objective.

CRED. PHISH

Credential phishing attacks designed to steal login access from users, employees, or partners via fake login pages, spoofed domains, or targeted spear phishing campaigns.

PAYOUT

Direct financial fraud targeting victims through scam campaigns, including wire fraud, LP distribution intercepts, fake investment schemes, and direct fan or investor payout scams.

BRAND/REP

Brand impersonation or reputation damage campaigns, including fake social accounts, counterfeit storefronts, crisis exploitation, and coordinated narrative attacks against an organization's public identity.

EXEC SAFETY

Executive impersonation and physical safety threats, including fake executive personas used to defraud employees or partners, and digital threats that escalate to real-world personal safety risks.

REC. FRAUD

Recruiting fraud using fake job postings, fabricated employee personas, or impersonated HR contacts, used to harvest credentials, extract fees, or conduct supply chain infiltration.

IP/COUNTER

Intellectual property theft or counterfeit goods operations, including fake product listings, unauthorized trademark use, and coordinated counterfeit distribution across e-commerce platforms.

* denotes an emerging or particularly acute signal within a vertical, indicating a threat pattern growing faster than the current security response and warranting elevated monitoring priority.

The Internet's Agentic AI Security Fleet

outtake

The Internet's Agentic AI Security Fleet