HUMAN AgenticTrust

Trust the agent. Control the interaction.

To keep pace with the rapid evolution of AI agents, organizations require new methods to verify agents, assess their intent, and govern automated interactions across digital surfaces.

AgenticTrust is a trust and governance layer for agentic AI. It enables organizations to detect and classify AI agents, verify trust level, and govern how agents interact with web and mobile applications. By evaluating the intent behind each agent-initiated interaction, AgenticTrust empowers businesses to enable high-value use cases, prevent abuse and fraud, and safely integrate AI agents into the customer journey.

According to Gartner®, "[by] 2035, 80% of internet traffic could be driven by AI Agents."

—Gartner Futures Lab: The Future of Identity, 7 April 2025[1]

[1]GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

AgenticTrust helps with

AGENTIC COMMERCE

AGENT INTERACTION AND GOVERNANCE

CONTROL OF AGENT ACTIVITY

REDUCING FRAUD AND ABUSE

DENYING SPOOFED OR MALICIOUS AGENTS

MONITORING AGENT BEHAVIOR

Benefits

DRIVE REVENUE WITH AI AGENTS

Enable verified agents to complete transactions and initiate interactions on behalf of users.

REDUCE RISK FROM AUTONOMY

Helps prevent fraud, abuse, and unwanted agent behavior that undermines trust, safety, or business logic.

UNDERSTAND AI AGENT BEHAVIOR

See the impact of AI agents on customer experience, policies, and application performance.

How It Works

COLLECTS
thousands of behavioral, technical, network, and reputational indicators

DETECTS
identifies and classifies AI agents with trust levels, requests, sessions and paths

CONTROLS
unwanted, excessive and restricted behaviors according to organizational needs

REPORTS
how AI agents interact with your platform and the route they take across it

ENABLES
new revenue streams from agentic commerce and interactions

Key Capabilities

Trust verification to assess if an AI agent should be allowed to interact with your applications.

Granular permission management e.g., deny access, allow reading, or checkout permission.

AI agent detection and identification including their name, provider, and agent type.

Fraud and abuse prevention by defending against spoofed or malicious agents and their activities

Real-time visibility showing intent, activities, session behavior, and top targeted routes.

Integration with HUMAN Sightline to provide holistic visibility, governance, and control across bots, humans, and AI agents.

The Human Advantage

Detection without Blindspots
We verify over 20 trillion interactions weekly across 3 billion devices, connecting global dots to reveal threats others miss across the customer journey.

Intelligence at the Core
Satori isn't just threat intel, it's a team on the front lines. From uncovering global fraud rings to surfacing new attack patterns, every HUMAN decision is powered by real-time insights.

Precision that Performs
>2,500+ signals per interaction. 400+ adaptive models. Decisions in milliseconds. HUMAN turns massive telemetry into high-fidelity decisions you can trust.