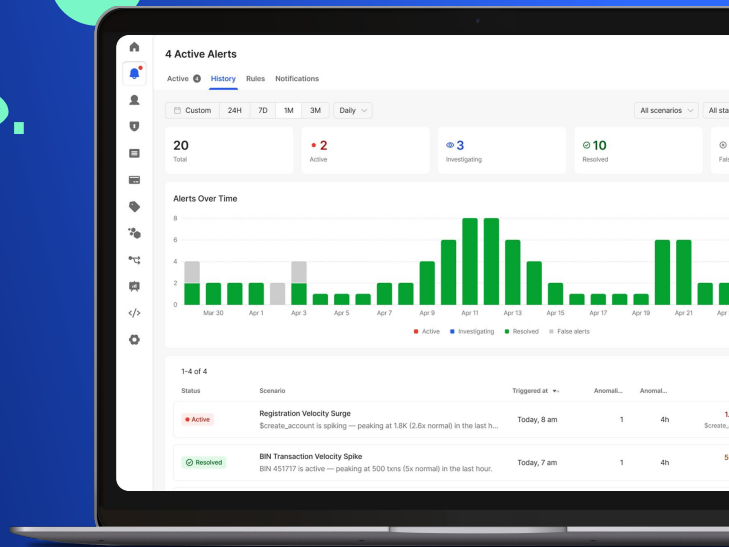




AI AGENTS SOLUTION BRIEF

Fraud runs at **AI SPEED**. Your analysts' tools should, too.

Sift's AI agents help fraud teams detect attacks, investigate users, review cases, and keep workflows tuned, so analysts spend their time on the decisions that matter.



THE PROBLEM

Attackers are automating campaigns at massive scale, while much of fraud prevention still runs on manual work.

Analysts piece together user histories across screens, review cases one by one, tune workflows by hand, and search documentation for answers. The gap isn't effort. It's speed.

Detect

Catch attacks as patterns shift, not after the damage.

Investigate

Get to the answer without piecing it together by hand.

Decide

Make the call with the evidence in front of you.

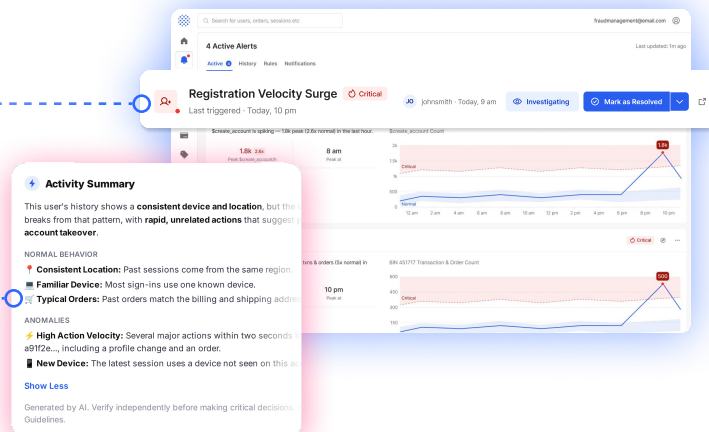
THE SOLUTION: SIFT'S AI AGENTS

Attack Detection Agent

Alerts your team when BIN attacks, order value anomalies, or chargeback spikes move outside your baseline, and pairs each alert with an investigation playbook. It's the first part of the Fraud Attack Defense Suite.

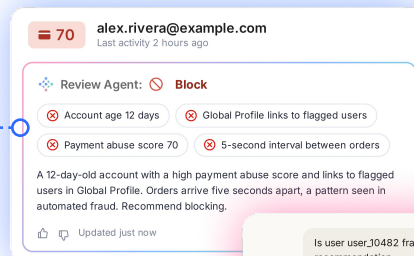
Risk Activity Agent (Account Defense)

Summarizes a user's behavioral history, shows what normal looks like for that user, and flags risky sessions, turning a 5 to 30 minute review into seconds.



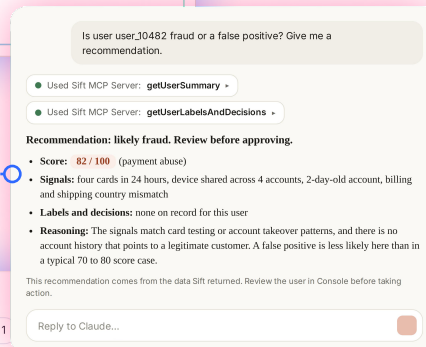
Review Agent (Payment Protection)

Surfaces key risk and trust signals, explains its reasoning in plain language, and suggests Block, Accept, or Watch.



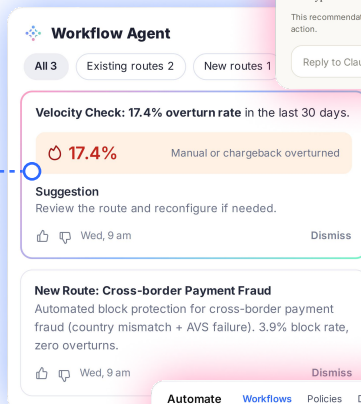
Sift MCP Server

Lets your own AI agent query Sift directly to investigate users and triage false positives from the tools your team already uses.



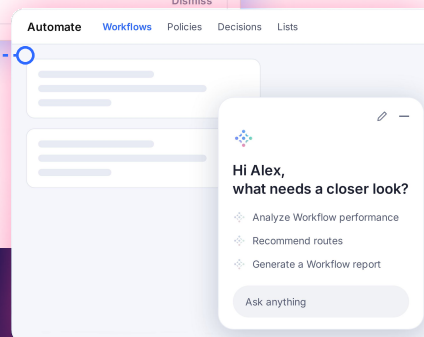
Workflow Optimization Agent

Optimizes your workflows against your traffic and recent trends.



Sift Copilot

An assistant built into the Console that helps analysts and integration engineers get answers and use documentation without leaving the page.



WHAT SETS SIFT APART

1

You chose the mode.

Every agent starts as an assistant, with your analysts making the final call. You decide, scenario by scenario, where to turn on automation, and you can change it as your needs change.

2

Built on a global network, not a generic model.

Workflow recommendations draw on best practices from Sift's cross-merchant network, so they aren't limited to what your own traffic can show.

3

Read-only access for your AI tools.

Sift MCP Server lets an agent see what your team can see, but not change a decision, label, or workflow.

Customer PROOF

In its first month, Attack Detection Agent caught a multi-hour, 20x transaction spike at a travel customer and a 13-hour card-testing surge at a retail customer, both attacks that would've run their full course the old way.

REQUEST A DEMO

sales@sift.com

