sift

Online Fraud Prevention: How rules-based systems are killing growth

Online businesses are constantly adapting operations and offerings to meet the changing needs of consumers. But behind every move that a merchant makes is a versatile fraudster ready to outmaneuver them, and exploit vulnerabilities along the customer journey with complex, sophisticated methods of attack.

Online merchants need to establish scalable fraud prevention strategies that don't undermine growth for the sake of protection. With a solution that effectively detects all types of abuse across a variety of channels, online businesses can enable their fraud teams to contribute directly to expansion—and give them the control they need to refine and scale fraud operations as the business matures.

With that in mind, merchants must consider whether a rules-based approach or a real-time, machine learning solution will be more effective at helping them meet both fraud prevention and revenue goals.

Machine learning (ML) instantly calibrates risk assessments based on new data and evolving fraud trends. It's the only way for merchants to achieve the accuracy required to drive online growth while stopping fraud before it happens —all while reducing false positives and lowering operational costs.

The Business Impact of Machine Learning Solutions

The efficiencies and accuracy afforded by machine learning solutions directly drive growth, stop more fraud, increase top line revenue, and improve customer retention by lowering false positives and eliminating the need for manual tuning.

Rules-based systems and strategies, however, focus on loss prevention, making them an impediment to growth and scale. They require significant operational investment to maintain, and restrict how quick and adaptable a fraud system can be—making it difficult to consistently identify fraud, eliminate friction points for trusted users, or mitigate evolving or unknown threats.

To effectively balance positive user experiences against accurate risk mitigation, optimizing the quality of every interaction has to be a priority. Machine learning is an ideal tool for growing online businesses—when fraudsters adopt new tactics or customers change behaviors, ML models ingest and analyze those signals in real time, automatically adapting risk thresholds to be more effective. This shrinks the number of trustworthy interactions that are inadvertently blocked or surfaced for review, and allows merchants to accept more orders while proactively stopping fraud.

With an ever-growing source of data feeding ML models, they're able to function a lot like a human brain—smarter with more information, and more effective over time.

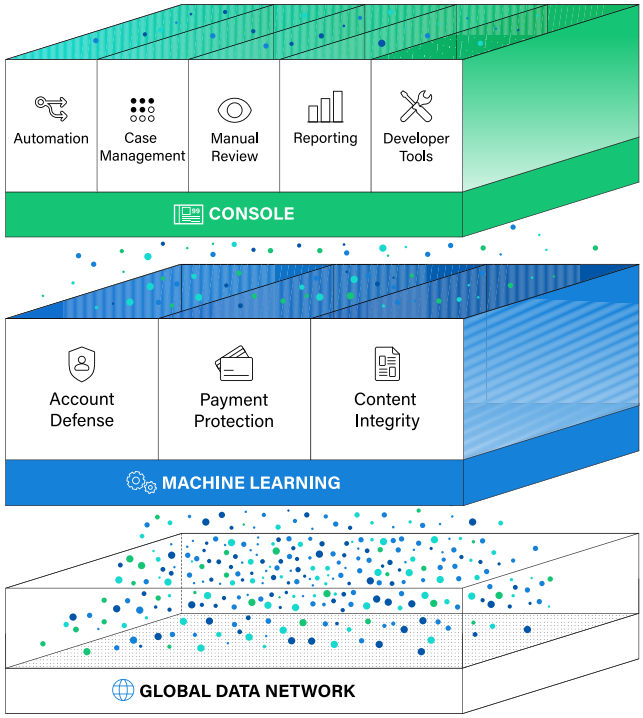
What to expect: Rules vs. machine learning

Business consideration	Rules-based systems	Machine learning solutions
Fraud operations *Does the solution address multiple types of fraud?* *How difficult will it be to integrate the solution into your current tech stack?* *Will ongoing engineering resources be required?* *How much manual input is required?*	Does precisely what is specified by fraud teams, who **must manually set risk thresholds to prevent known, recurring fraud attacks (but cannot detect changing or emerging fraud).** **Major changes to risk thresholds and rules require engineering resources.** **Human input is necessary** to adjust the system when new data is presented.	Feedback automatically influences models for **continuously-improved accuracy and scalability.** Unique models can be developed for different fraud types. Support for multi-channel transactions. Simplifies exporting data to new channels, systems, and tools **(no developers required).**
Data input *How accurate is the solution?* *How robust are the solution's data mining, ingestion, and output capabilities?*	Requires manual tuning to adapt to new data. **Accuracy goes down over time as user behaviors and fraud tactics evolve.** Limited scalability—**human input and thresholds must be regularly readjusted to meet new demand and increasing fraud.**	Real-time risk assessment and data updates. **Accuracy improves over time as more data is ingested and models are refined.** Infrastructure to support large data spikes/fluctuations and scale with growing operational needs.
Customer impact *Can the platform address your unique fraud prevention needs without sacrificing growth or customer experience?*	Trusted users can exhibit signals associated with fraud (high velocity or login from a new location) while risky users can fail to trigger rules based on known patterns. **This results in high false-positive and false-negative rates.**	**Fraud is stopped in real time**, because ML models recognize a multitude of risk signals simultaneously and in milliseconds. **Streamlines the user experience by tailoring friction** and only applying it when required. **Enables frictionless experiences** like one-click checkout, increasing customer LTV and improving brand loyalty.
Scalability *Can the platform scale with the business as it grows?* *As the business expands, what impact will investing in this solution have on fraud operations and other areas of the company?*	Rules and risk thresholds can be manually set right away, but require **reactive adjustments.** **Rules expire, and are quickly rendered inaccurate** with changes in customer or fraudster behaviors—leaving risk teams unable to catch up. Launching in new markets creates risk that's difficult to mitigate with rules, which **can't adapt in real time to stop unknown fraud.**	Flexibility and customizability to support current and future business needs and volumes. Adapts in real time**, effortlessly scaling alongside the business** to enable growth while preventing known and unknown fraud. Requires some time for data ingestion to train ML models. **Becomes more accurate, efficient, and intelligent with every data point served.**

How Sift Works: The mechanics of Digital Trust & Safety

Sift allows trust and safety teams to proactively prevent fraud, streamline operations, and grow revenue using an integrated solution that stops multiple types of fraud, including account takeover (ATO), payment fraud, and content abuse (spam and scams).

An intuitive Console puts analysts in control with powerful automation, case management, and real-time reporting, while an ensemble of machine learning models provides the highest accuracy in the industry: Sift customers have cut fraud by 80% or more and saved hundreds of hours previously spent on manual review. With learnings from the 60B events processed by Sift's global network every month, businesses can stay ahead of evolving trends and attack vectors—including those that have never shown up on a merchant's website in the past.



Sift helps us enable decisions with much higher confidence. The Sift Score is a benchmark for us to decide on fraud investigations. Today, we process tens of thousands of transactions each month and it only takes a few days to see statistical relevance. Sift helps make it very accessible to fight fraud on a world-class level.

Remitly

Nate Spanier
Director of Operations, Remitly

Contact Sift today for a deeper dive into our technology, and to explore how your business can stop more fraud and catalyze growth with Digital Trust & Safety.

End-to-end intelligent automation with Sift

Sift is the leader in Digital Trust & Safety, empowering companies of every size to unlock new revenue without risk. Our cutting-edge platform dynamically prevents all types of online fraud and abuse with intelligent automation that adapts based on Sift's unrivaled global data network of 70 billion events per month. Global brands including Twitter, DoorDash, and Wayfair rely on Sift to catalyze growth and stop fraud before it starts.

Visit us at sift.com and follow us on LinkedIn.

© 2022 Sift Science, Inc. All rights reserved. Sift and the Sift logo are trademarks or registered trademarks of Sift Science, Inc.