

Digital Trust & Safety Vendor Evaluation Checklist: Machine Learning vs. Rules











How to Use This Evaluation Matrix

With Digital Trust & Safety, businesses can align risk and revenue decisions by fundamentally evolving their fraud prevention strategy, from mindset and processes to technologies and platforms. By using real-time machine learning, as well as data from merchants and markets all over the world, this cutting-edge approach to fraud prevention gives you the ability to accurately separate suspicious behaviors from legitimate ones in less than a second—all while enabling you to deliver superior experiences to trusted users and stop fraudsters from undercutting your revenue. It's machine learning you can actually count on.













As you explore Sift as your new Digital Trust & Safety solution or compare it to your current fraud prevention platform, we suggest considering the following questions:

- Does the solution address multiple types of fraud?
- How robust is the Sift global network compared to what you currently have access to?
- Can you tailor the model to your unique business needs without sacrificing growth or customer experience?
- Can you improve the user experience using Sift's models?
- Can the platform expand a single data point into multiple fraud signals for better accuracy, or will you have to manually build it out on your own?
- Does the solution include manual review tools?
- How difficult will it be to integrate into your current tech stack?
- Will you require ongoing engineering resources to respond to new attacks?
- How robust are the reporting features compared to your existing outputs?
- What kind of support can you expect from the vendor?
- What is the uptime?
- How quickly does the model adapt to and catch new fraud patterns?

Below, we've outlined the most critical technology capabilities, security features, reporting options, and support needs your business deserves to actively predict and prevent fraud, protect and delight customers, and grow your business.

Feature or capability	Sift	Current platform
Technology		
Real-time risk assessment at every interaction (e.g., account creation, transaction, login, content creation) and real-time, global data network updates		
Support for unlimited custom data and custom, user-designed fields – including unique events and specific features and signals		
Multi-channel support including web, mobile, and BOPIS/BORIS transactions		
Robust feature engineering* to extract more signals from individual data points		
<small>* Feature engineering is the process of transforming raw data into features that better represent the underlying problem to predictive ML models, resulting in improved accuracy.</small>		
<u>Ensemble of models</u> deployed for comprehensive and accurate risk assessment		
Online learning—model automatically updates within milliseconds with new user interactions		
Global network model that shares learnings across customers in real time to boost accuracy		
Unique models for different abuse types including fraudulent payments, account takeover, and spam content		
Dedicated custom model which incorporates custom features and learns fraud patterns specific to your business		
Supervised model that allows feedback to automatically influence the model for improved accuracy		

Feature or capability	Sift	Current platform
Platform Console and Integration		
Web-based console with case management capabilities including built-in queues and user/order level views	✓	
Link analysis including visual interface to show users connected by device, IP, etc.	✓	
Rule-building capabilities that allow deployment without developer resources	✓	
Infrastructure to support large bursts or fluctuations of data (e.g., online traffic spikes due to seasonality) and scale with growing operational needs	✓	
Internal controls to configure and assign multiple roles and permissions—including customizable ones	✓	
Integrates seamlessly with your existing fraud stack with the flexibility to input different types of data from multiple sources, and output to other existing systems	✓	
Offers the flexibility and customizability to support current and future business needs and volume	✓	
Provides the necessary scalability to support current and future business needs and volume	✓	
Makes it easy to export data to new channels, systems, and tools	✓	

Feature or capability	Sift	Current platform
Security		
Data encryption at rest		
SOC II certification		
Support for mandatory 2FA and SSO to grant access to user console		
Provides governance and access control, user management, and compliance of customer data		
Reporting Capabilities		
Pre-built reports analyzing order and chargeback metrics (e.g., order volume, accept rates, block rates, chargeback rates, etc.) in real time		
Pre-built reports to monitor team performance (e.g., number of cases reviewed, review accuracy, etc.)		
Pre-built reports to monitor rule effectiveness		
Ability to easily export reports to CSV for further data analysis		
Partnership and Support		
Dedicated Sales Engineer for integration planning and deployment		
Dedicated Technical Account Manager for onboarding, training, and continued support		
Access to Trust and Safety experts for consultation on building a holistic strategy		
Additional channels for technical support, troubleshooting, and additional questions or concerns		

Find out how your business can benefit from a Digital Trust & Safety strategy by taking our [online assessment](#).