Arkose Labs

BUYER'S GUIDE TO FRAUD & ACCOUNT SECURITY

7 CONSIDERATIONS FOR DIGITAL BUSINESSES

EBOOK

A NEW FRONTIER IN ACCOUNT SECURITY & FRAUD PREVENTION

With the evolving attack patterns targeting websites, apps and digital platforms, businesses must ensure their fraud detection and account security technologies are up-to-date and secure. Choosing a third-party vendor to provide these services can help businesses save costs and increase their ROI. Although building these tools internally may require more resources, having access to the latest technologies and a team of experts can help businesses stay ahead of the changing threat landscape.

THE BUILD VS BUY DEBATE

Price: The upfront cost to build a solution in-house may be less expensive, but will suck time and internal resources to build and maintain, often leading to a higher overall cost.

Data: Effective fraud prevention demands large datasets to test and refine models. Internal solutions access targeted customer data, whereas external vendors offer valuable network data.

Analysis: With how fast attack patterns change, fraud and security teams need solutions they can confidently rely on. Accuracy in risk signals and transparency both play an important role in reducing manual analysis.

Time: Internal tools take a long time to develop and implement. SaaS solutions provide more rapid results, but can take time to fine-tune to bespoke needs.

1. ADVANTAGES OF WORKING WITH A VENDOR

The right account security vendor will offer a cost-effective, efficient service that benefits from shared threat data across their network. In the ever-shifting threat landscape, it is critical to identify and stop new types of fraud early in the process to prevent serious damage downstream. A third-party vendor does the heavy lifting in the development lifecycle and customers benefit from their previous experience in deploying the software.

There are also budget considerations: internal projects are often subject to ballooning costs based on factors such as economic fluctuations, evolving business goals and regulatory involvement. Partnering with a vendor can save money and alleviate some burden on internal fraud and security teams, leaving them to focus on strategic tasks and achieving a stronger ROI.

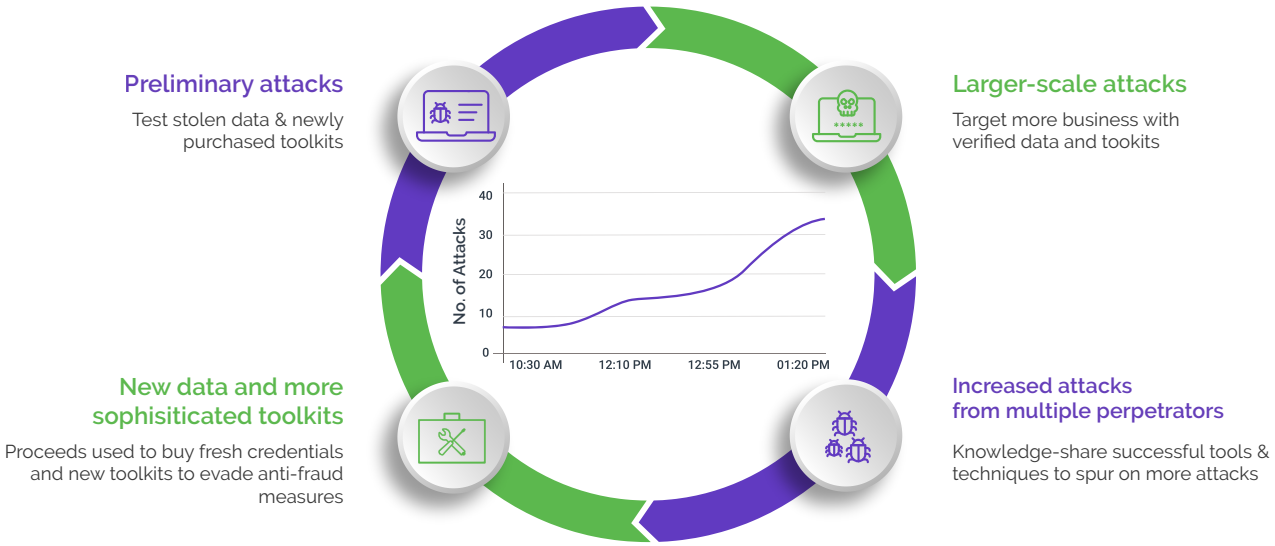
Key questions to ask:

- Is the platform able to monitor attacks across its entire network, and therefore constantly adaptive to evolving threats?
- Is the product user-friendly and can the vendor roll it out rapidly for immediate benefit?
- Does the platform offer a data network effect driven by the shared insights across the vendor's client base?
- Does the vendor's package and team complement the in-house talent?

2. NOT ALL SOLUTIONS ARE EQUAL

Businesses looking to prevent fraud and secure their accounts should be aware of the vast array of solutions available on the market. Making the right choice can be difficult when there are so many options of varying degrees of effectiveness and cost. Making an informed decision can help to maximize savings and ensure a positive ROI. Careful consideration should be taken before entering into a lengthy contract and partnership, to ensure that businesses get the best possible return on their investment.

The fraud attack spectrum is diverse; while the majority of fraud attacks continue to be carried out by bots, there is a marked trend of increasing human-driven attacks, along with a continued evolution in the automated tools that are used to circumvent anti-fraud controls. Then there are highly skilled lone fraudsters who launch targeted attacks against carefully chosen targets with a high potential for monetization. A good fraud solution should be able to defend against all types of attacks and save you money in the long-run.



3. FOCUS ON BUSINESS OUTCOMES AND NOT ON CAPABILITIES

Perhaps no issue is as important as this one. Vendors can tout features and functionalities, but what does this mean for businesses in practical terms? Ultimately, in working with any vendor, the end goal is to increase ROI, keep existing customers happy and attract new ones.

Finding the right vendor for fraud prevention can be daunting, but the cost savings associated with a trusted and reliable provider can be immense. Look for a vendor that can help streamline operations and provide the best security for your business without compromising on customer experience. Doing your due diligence and finding the right vendor to fit your business's needs will result in significant savings down the line.

Some questions to consider:

- Is the service compatible with, or will it enable the company's business objectives?
- Do the design and functionality add value to the overall solution, or are there superfluous, clunky features?
- What are the long-term cost savings associated with using the service?
- Will the solution align with internally established fraud detection KPIs?
- Can it meet the criteria set out by internal stakeholders across the businesses who will be impacted by the solution?

4. ADAPT TO THE ENTIRE ATTACK SPECTRUM

Bot attacks are more sophisticated and harder to detect than ever before, and they are getting more advanced by the day. At the same time, human-based attacks are on the rise, as fraudsters hire sweatshops groups of low-paid human workers who carry out attacks at scale to do more nuanced tasks such as leaving fake reviews, upvoting and downvoting videos, or sending malicious messages.

The optimal solution should be able to adapt to the entire fraud attack spectrum while ensuring genuine customers have a smooth user journey.

Key questions to consider:

- Does the solution have the capacity to accurately classify and identify traffic based on risk? If so, can it differentiate between automated and human-driven attacks?
- Can the platform utilize rich data intelligence and powerful analytics to move beyond traditional risk scoring and provide powerful indication of intent in real time?

- Are genuine customers offered a clear path to remediation, with tailored authentication challenges presented to high risk traffic?
- Can the solution scale up to handle large volumes of traffic without requiring more resources?
- Will the strategy offer clear actionable insights, beyond the binary 'good' versus 'bad' traffic, and detailed analysis of attack patterns?

5. IMPACT ON USER EXPERIENCE

A good platform should be built foremost with customer experience in mind and deliver enhanced fraud detection and lower operational cost without impacting good customer throughput rates. Good customer throughput can be enhanced through better detection and user-friendly enforcement.

Most businesses struggle with finding that "sweet spot" between being vigilant to bot and human-driven attacks and creating a seamless digital experience for genuine customers. By using a solution that utilizes intelligent friction, it ensures good users are able to breeze through while the bad guys are shut out.

A Zero Trust Approach

It's imperative that organizations take a zero-trust approach to data. Fraudsters have by and large cracked the code, so to speak. They know the parameters that companies use when taking a risk-based authentication approach, and are able to circumvent many fraud mitigation solutions at scale. This means not implicitly trusting any data and device characteristics coming into a website, since digital identities are limited in scope. Fraudsters can easily change their source IP addresses, spoof legitimate customers' devices, hide their true location, and so on. For long term fraud prevention and real cost savings, use a solution that offers powerful secondary screening to root out fraudsters while allowing true customers to prove they are legitimate, resulting in a more robust ROI.

Key questions to ask:

- Is secondary screening targeted according to risk profile?
- Are they resistant to the latest innovations in machine vision technology?
- Are the challenges fun and easy to complete ensuring high throughput rates for good customers?
- What cost savings can be expected by implementing this solution?

6. TIME TO VALUE

Choosing a fraud vendor is only half the battle. After that comes onboarding and implementation, which can be an arduous process. Some vendors have very specific requirements in terms of technology and usage, and some may require integration of on-site hardware. Complicated implementation processes mean that it could take many months from signing a contract to actually seeing the results of a solution in action. This can impact time to market and how soon customers benefit from the new service. A quick time to market is a main reason to work with a vendor as opposed to building a tool internally, so a long implementation process can greatly impact ROI.

Key implementation questions to ask your fraud vendor:

- How fast can we onboard the solution and see an impact?
- Where in our tech stack will it fit and how does it integrate?
- Can the server-side aspects be integrated into existing infrastructure?
- What potential cost savings do we stand to gain from implementing this solution?

7. A TRUE PARTNERSHIP

Technology, though important, isn't everything. Without good customer support and insights into trends and patterns, companies may be left fumbling with a product they are not sure how to use to its optimal ability.

That's why cutting-edge technology must also be combined with a robust managed services offering that can give deep insights into attack data and work directly with clients to remediate any and all fraud attacks. By taking this approach, businesses can realize cost savings in their fraud prevention efforts, while receiving a level of customer service that feels like an extension of their own internal team.

Questions to ask your potential vendor-partner:

- Do they have a customer support team that is available round the clock to respond to any queries?
- Is their team made up of talented and dedicated people with deep industry experience?
- Can they offer customizable solutions and a deep knowledge of specific business needs?
- Do their SLAs stand behind the quality of the product?

Lean on Expertise

A digital business has many priorities: Innovative new products and services, helping customers meet needs and generating revenue. For many companies, their main area of expertise may not be fraud prevention. That is another critical reason to work with a vendor partner. They can bring expertise from helping a wide range of clients stop fraud and experience from defending against many types of fraud attacks. A quality vendor will also share ideas and suggestions that internal teams may have never considered, that ultimately will improve efficiency and reduce costs

CONCLUSION

When it comes to investing in fraud prevention and account security solutions, every company must weigh up whether to work with a third-party vendor or build a solution of their own. Working with a vendor partner brings a number of benefits, including access to network intelligence and insights, ability to quickly scale up or down as needed, a quick implementation and roll out, and much more.

Perhaps most importantly, an account security vendor's core purpose is protecting accounts from being compromised. A good vendor can act as an extension of a business's internal fraud and security team and take care of much of the heavy lifting associated with identifying and stopping relentless fraud attacks on a daily basis. These are experts with deep knowledge and experience in identifying and stopping fraud who can ensure the safety of any digital business platform and its users.

Choosing the right fraud vendor is imperative, as making the wrong decision can end up costing a lot of money and time in the long run. Selecting a secure and reliable fraud solution can lead to cost savings and a far better ROI. In a world where business is done digitally more than ever before, and fraud attacks are more frequent and severe than ever, it is crucial to find a partner that can help stop bad guys at the front door while maintaining a great user experience for customers and saving long-term.

Arkose Labs

Arkose Labs undermines fraud to stop bad actors. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the motivations behind attacks, while improving good user throughput and offering considerable savings. Based in San Francisco, CA with offices in Brisbane, Australia and London, UK, the company was honored as the 195th fastest growing companies in the United States on the 2021 Inc. 5000 list.

Mail:

support@arkoselabs.com

Address:

USA • 250 Montgomery St, Fl 10, San Francisco, CA. 94104

Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006

United Kingdom • 167-169 Great Portland Street, 5th Floor, London, W1W 5PF

Schedule Demo