Arkose Labs

6 Key Pillars
of Future-Proof Attack Detection

EBOOK

SECURING THE DIGITAL FRONT-END FROM EVOLVING ATTACKS

The abundance of digital channels available today is a boon for businesses, who now have numerous avenues to connect with consumers. But the downside is that it also means attackers have numerous touchpoints to target for fraud and abuse.

Nearly all industries have seen a rise in attacks across their digital front-end - despite significant investment in talent and technology. Account security, has become a major security issue for digital businesses. There was an 85% increase in attacks targeting the login and registration points on the Arkose Labs Global Network in 2021.

Attackers are adept at bypassing enterprises' fraud and anti-bot defenses - any new security measure we put in place will lead to evasion attempts and countermeasures. This risks a perpetual game of cat-and-mouse between businesses and attackers.

THE BUSINESS IMPACT

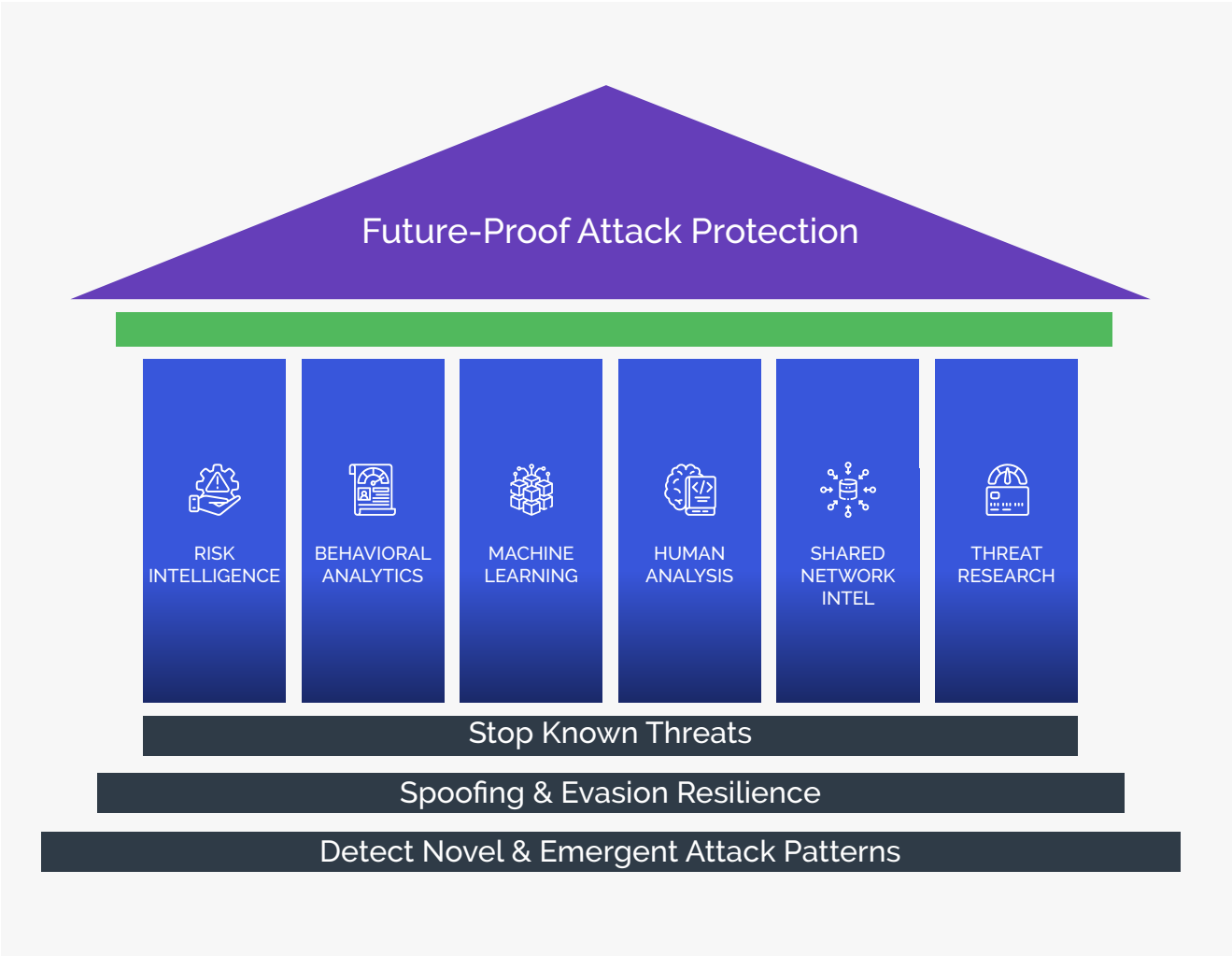
This game is costly to businesses. It is hard to get visibility into attacks, as attackers randomize attacks and deliberately display inconclusive signals. This leads to false negatives, where attacks are let through - or false positives, with good users being caught up in security controls.

Periods of intense attacks also put a strain on internal fraud and security teams, who are constantly fighting fires.

- Lack of visibility into attacks
- Strain on fraud & security teams
- Impact on good user experience

THE 6 PILLARS OF FUTURE-PROOF ATTACK DETECTION

To keep ahead of evolving threats, businesses need a defense-in-depth approach to fraud prevention and account security. They need graduated security measures which identify and stop known threats based on previous attack signatures; ensure dedicated controls to assess for spoofing and evasion techniques; and carry out sophisticated machine learning and human analytics to identify novel and evolving attack patterns.



#1 ACTIONABLE RISK INTELLIGENCE

Businesses, especially large, global enterprises, likely have access to quite a bit of data. But just having large amounts of data is not enough, businesses need to be able to connect the dots to make faster decisions. That means being flexible and open to evaluating new signals as they emerge and incorporating them into their detection engine. It's imperative to be constantly adding new insights.

Key data points businesses should be looking at include identifying device and network characteristics and geography. They also need to analyze historical traffic patterns, which can help identify and detect traffic anomalies that can indicate attacks.

This helps not only to identify potentially bad traffic coming to a site, but also ensures good users do not get misidentified and caught up in the security web. False positives lead to customer frustration and customer churn. Ultimately, it is important to have a critical mass of robust data in order to detect the nuanced risk signals inherent in today's sophisticated attacks.

#2 BEHAVIORAL ANALYTICS

Robust analysis of user behavior using both behavioral biometrics and behavioral analytics is also effective in detecting bad bots vs. good users vs malicious humans.

While behavioral biometrics looks at the way a user interacts with a device, like mouse motions, keystroke dynamics, or touch screen interactions, the behavioral analysis looks at what a user interacts with in a web service and gives context to the actions they take. The key is to analyze enough behavioral data in order to spot outliers and anomalies in the patterns. This information, taken together, gives a holistic look at traffic and identifies signs of bad behavior.

Collecting this data can help detect attacks in a way that is independent of IP or device information, so when each dataset is combined it leads to a much stronger detection signal.

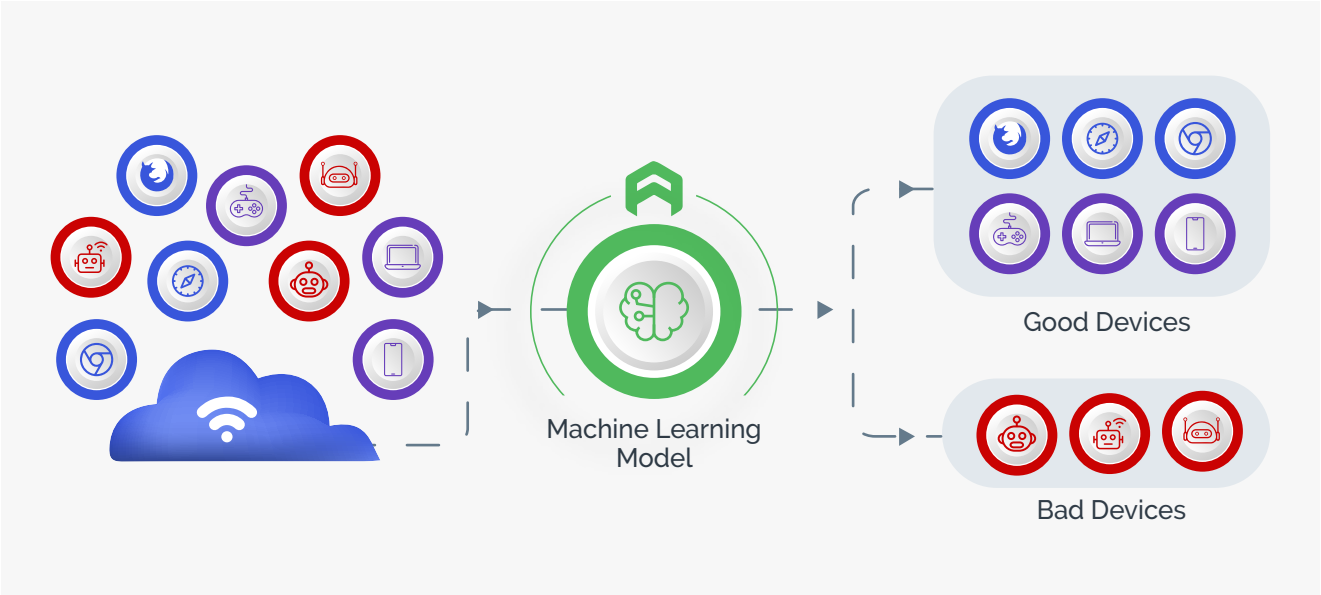
Behavioral Biometrics	User Behavioral Analysis
Desktop & laptop: Mouse and key press events 	
Mobile device: Touch event, accelerometer, gyroscope	

#3 LEVERAGE MACHINE LEARNING

Machine learning is vital to parsing and analyzing signals in vast amounts of data. It enables businesses to accurately correlate disparate risk signals, and weigh different attributes to correctly classify and assign a risk score.

ML plays a key role in anomaly detection, which is the process of identifying deviations from the majority of data in a set of patterns or behaviors considered standard events. These deviations may be suspicious, unusual, or rare. Anomaly detection helps identify critical incidents that need attention to resolve problems or gain insights into ongoing processes to make improvements.This also helps inform traffic shaping and predictive analysis of traffic patterns.

Using machine learning businesses can also automatically update rules based on newly identified attack patterns to protect across use cases and different lines of business.



#4 HUMAN ANALYSIS & OVERSIGHT

Of course, machines can't do everything, and analysis and insight from experience, trained security professionals is also needed. Security operations analysts are vital in the day-to-day analysis and monitoring of traffic. They help adapt to evolving attack patterns and investigate risk signatures identified by machine learning algorithms.

During key events of expected heightened traffic, human analysis is necessary to examine intricate patterns, as attackers often use these events to hide amongst good traffic. Human analysts also proactively monitor for anomaly detection to keep a watchful eye on traffic and proactively flag potential threats.

#5 SHARING NETWORK INTELLIGENCE

No company is an island, and most bad actors launch similar attacks targeting many companies at the same time. That's why having access to shared network intelligence or consortium data from other businesses is vital. Shared intelligence helps businesses more effectively identify attacks that others have already seen. Sharing data on attack patterns across use cases and industries can greatly help intelligence gathering and detecting attacks.

Of course, any data shared between businesses must be anonymized to maintain privacy. This is most easiest done with a vendor solution. Working with a vendor that has a robust clientele across industries and around the globe means that each business that works with it benefits from this combined intel.

#6 THREAT INTELLIGENCE FROM THE DARK WEB

Powerful threat intelligence is the backbone behind any good detection engine. This means actively tracking known fraud operations, including visiting the channels where they communicate in order to learn about tools and techniques they use.

Threat intel means not only observing bad guys, but going deep into their world, infiltrating dark web forums and communities on platforms such as Telegram. This can also have the benefit of turning fraudsters into "white hats" by engaging with them. Companies can, for example, pay them money for insight or intelligence on how they launch attacks.

THE ARKOSE LABS APPROACH

Arkose Labs believes businesses need to be armed with a combination of real-time risk decisioning, machine learning, and human analysis, to uncover high-risk activity in real-time, while optimizing rapidly with attack patterns. This defense-in-depth approach provides long-term deterrence for fraud and security teams.

Arkose Detect, our proprietary detection engine, empowers security and fraud teams to root out large-scale, persistent attacks, with real-time risk classifications of traffic, powered by multi-faceted machine learning and 24/7 analysis from a Security Operations Center. The detection engine uses a combination of rate limiting, IP and device intelligence, traffic shaping, and behavioral biometrics that ensure attacks never go unnoticed.

Unlike other black box solutions, our transparent approach focuses on delivering actionable insights, with a clear path to remediation. Customers benefit from clear explanations for risk classifications and we share 70+ raw data fields from each session. We leverage insights from across our global network of historical attack patterns to asses traffic in real time, and decipher between good and bad traffic with maximum accuracy. This allows companies to keep the occurrence of false positives and negatives to a minimum.

THE ARKOSE ADVANTAGE

Actionable insight - Transparent detection gives businesses superior insight data to enhance risk models. Our detection capabilities allow for a stronger security posture and offer flexibility in response technique.

Simple and easy deployment - Arkose Labs is the fastest enterprise-ready risk detection available on the market, with businesses seeing actionable insights within days, rather than months.

Partners in your success - Other detection solutions take lots of internal resources to implement, tune & monitor. Arkose Labs does that for you. Our 24/7 SOC is there to help assist your internal teams at all times.

Global network - Arkose Labs customers benefit from the data network effect driven by the shared insights across the Arkose Global Network, derived from more than 60 clients around the globe across dozens of industries.

CONCLUSION

Unfortunately, there is no one silver bullet for accurately detecting fraud attacks. Bad actors constantly revise and refine their tactics. But by taking a defense-in-depth, layered approach, businesses can be assured they are taking the past route to detecting and stopping attacks.

Using all the data businesses have wisely in order to make sense of traffic patterns and spot analogies is key. This should also be combined with best-in-class vendor technology along with third-party professional services to help augment internal talent. With this in place, digital businesses can be confident in their ability to detect even the most advanced attacks coming to their platform.

Arkose Labs

Arkose Labs' mission is to create an online environment where all consumers are protected from malicious activity. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication," the company offers the world's first $1 million credential stuffing warranty. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks while improving good user throughput. Headquartered in San Francisco, CA with offices in Brisbane and Sydney, Australia, San Jose, Costa Rica, Tokyo, Japan, and London, UK, the company debuted as the 83rd fastest-growing company in North America on the 2021 Deloitte Fast500 ranking.

Sales:
(800) 604-3319
Mail:
support@arkoselabs.com
Address:
USA • 250 Montgomery St, Fl 10, San Francisco, CA. 94104
Australia • 315 Brunswick St, Fl 2, Brisbane, QLD. 4006
UK • 167-169 Great Portland Street, 5th Floor, London, W1W 5PF

Schedule Demo