Arkose Labs

Arkose Labs Helps Multinational Bank Enhance Consumer Experience and Defeat MFA Compromise

KEY RESULTS

Reduced false positives, improving the experience for genuine users

Enabled robust data sharing, offering high transparency into attack traffic

Identified and mitigated a massive number of phishing domains

SUMMARY

A large global financial services company serving customers in more than 30 countries faced frequent disruptions caused by false positives from anti-fraud measures designed to combat sophisticated bot attacks. The bank's fraud prevention solution was frustrating legitimate users, especially high-net-worth individuals, making account login increasingly cumbersome. This disrupted access to critical services and eroded trust in the bank's digital offerings. Additionally, the solution provider was not supplying the necessary transparency for the bank to fully understand its traffic and implement improvements.

The financial institution sought a true partner in combating cybercrime and access to valuable risk signal data to feed into its internal models. When the bank reviewed the Arkose Labs solution, it quickly recognized Arkose Labs as the ideal partner for securing its consumers' online accounts from scams and fraud while enhancing the digital banking experience consumers expect. Additionally, the Arkose Labs 24/7/365 SOC detected nearly 50 active phishing domains that were previously unidentified, thus protecting the bank from possible reputational damage.

THE BUSINESS PROBLEM

Picture yourself as the CEO of a leading global bank. You attempt to log into your online banking account and are unexpectedly required to pick all the squares that contain a motorcycle (or something similar)—not just once, but twice and maybe even three times. Now, consider the frustration of your high-net-worth clients experiencing the same problem.

This real-world challenge highlighted a deeper issue: The bank was grappling with growing customer dissatisfaction, particularly among its elite clientele, who found the account login process increasingly burdensome due to legacy security tools. The root of the problem lay in the anti-fraud measures, which, while aiming to thwart sophisticated bot attacks, were generating numerous false positives. This reality not only disrupted access to critical services but also undermined trust in the bank's digital platforms. The bank urgently required a solution that would provide deeper visibility into suspicious traffic while improving its account security and bot detection and mitigation strategy, ensuring robust fraud protection without disturbing the experience of its most valuable customers.

THE ARKOSE LABS SOLUTION

The Arkose Labs solution provides financial institutions with modern technology to detect and mitigate sophisticated attacks orchestrated by bots and human fraud farms—before they make impact.
Monitoring more than 227 risk signals, the Arkose Labs platform significantly reduces problem traffic at the top of the funnel. It leverages behavioral biometrics to accurately detect and stop attacks, while its adaptive challenge-response suite triages suspicious traffic, allowing genuine customers to proceed without issue.

In the early stages of deployment, Arkose Labs integrated its solution into the bank's account login flow, which handles about 90% of the bank's traffic. By analyzing nearly 100 million sessions over several weeks, Arkose Labs demonstrated the platform's robust detection capabilities.

The bank sought more detailed risk intelligence and data to enhance decision-making accuracy and appreciated Arkose Labs' commitment to transparency and explainability. The Arkose Labs platform provides real-time detection and mitigation insights that surpassed previous solutions, offering visibility into factors such as VPN usage, proxy connections and geographical locations. Additionally, the platform excels in advanced detection techniques, including browser and device fingerprinting and anomaly detection.

For instance, if a user logs in from an iPhone 14 using Safari, the Arkose Labs solution performs an in-depth analysis of the device. Any anomalies, such as an unusually large screen resolution or unexpected browser add-ons, trigger alerts and the system transparently communicates these findings to the bank.

Arkose Labs' commitment to delivering comprehensive explanations for why a session was flagged as suspicious, including the relevant risk signals and the rationale behind the challenges presented, helped the bank better understand false positives and fine-tune its defenses.

Furthermore, the Arkose Labs solution integrates directly into the application's login flow, conducting data analysis inline without rerouting traffic. This seamless integration minimizes perceived latency for users, unlike solutions that require multiple round trips of traffic between the front end and their cloud. The globally distributed infrastructure supports large enterprises with worldwide customers by analyzing traffic locally, avoiding delays associated with sending data across continents.

As an added value, Arkose Labs brought unique capabilities in the form of real-time detection and mitigation for reverse proxies used in MFA compromise. In this type of attack, an attacker sets up a reverse-proxy server that masquerades as the legitimate company website, leading users to believe they are logging in directly. When users enter their credentials and the MFA one-time passcode (OTP), attackers capture both the credentials and the OTP, allowing them to take control of the account.

Arkose Phishing Protection detects these phishing attempts by leveraging a unique integration model to combat this MFA compromise effectively. As part of the deployment strategy, the solution inspects every login request and requires a valid Arkose Labs token for authentication. This requirement extends to reverse proxy phishing attacks, which are required to still generate valid Arkose Labs tokens for every session to gain access.

Therefore, those conducting phishing attacks need to include Arkose Labs within their workflow, allowing Arkose Phishing Protection to collect critical intelligence. This integration facilitates the real-time detection and blocking of phishing sites, and it can be used to support formal takedown requests for the identified phishing domains.

Conventional tools, on the other hand, fail to categorize these sites due to their short-lived nature and rapid domain changes.

DEMONSTRATED RESULTS

The bank swiftly identified Arkose Labs as the perfect ally in protecting its customers' online accounts from scams and fraud, all while improving the digital banking experience that its consumers desire. Through two rounds of fine-tuning for false positives, the Arkose Labs solution is effectively aiding the bank in minimizing unnecessary challenges for legitimate users.

For a major bank with over 70 million customers and a complex infrastructure, implementing new technologies and workflows requires careful handling. The bank is now in the process of rolling out the platform across its mobile and web login flows, where the platform is expected to prevent between 1 to 5 billion attack sessions per year. With bank-grade compliance and certifications, Arkose Labs is streamlining the process, supported by an agile and responsive team throughout.

Remarkably, Arkose Phishing Protection identified nearly 50 active phishing domains within just four days of the bank's implementation, a significant number that indicates high interest from the cybercrime community in defrauding the bank's clients. These phishing sites are part of sophisticated social engineering scams deployed by fraudsters and can have a negative financial impact on the bank as well as severely damage immediate customer trust and the longer-term customer relationship if left undetected. This proactive approach ensures that phishing threats are addressed swiftly and effectively, outperforming traditional, less agile detection methods.

Arkose Labs also helps banks see the bigger picture of the fraud landscape by providing intelligence on evolving threats and fraud trends. The Arkose Global Intelligence Network, a consortium that allows Arkose Labs customers to benefit from data on global risk signals, mitigation, and other observations about the changing threat landscape, is based on data gathered by the company's world-class threat research team combined with its SOC.