WHITE PAPER

The Economics of Account Takeovers in Banking: A Tipping Point

The numbers behind the attacks

CONTENTS

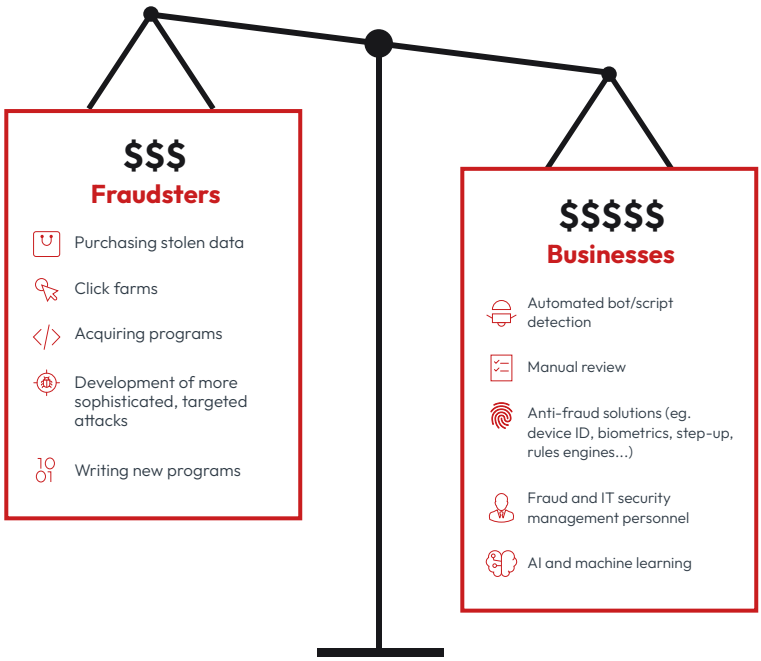
Executive Summary

Account takeover (ATO) attacks represent a significant and growing threat to the financial services industry, driven by a highly profitable business model for cybercriminals. Data from the TransUnion 2023 State of Omnichannel Fraud Report indicates an 81% surge in ATO fraud over the previous four years,[1] emphasizing the urgency for robust security measures. This white paper, "Economics of ATOs in Banking," meticulously breaks down the numbers behind these attacks. It examines the economic dynamics, supported by the latest market data, to illustrate the significant impact on both the attackers and the financial services institutions. The paper highlights how advanced security measures are crucial in making these attacks financially unviable for cybercriminals.

Factors Influencing ATO Revenue

Although ATO attacks have been a challenge for over two decades, their persistence is due to the constantly evolving tactics of attackers, who continually refine their methods and leverage sophisticated automation and human deception that make it difficult for defenses to keep pace. The income from these attacks hinges on several factors: the hit rate of stolen credentials, the attacker's reputation and the market price of stolen accounts.

1. Hit Rate: The effectiveness of an attack is partially determined by the hit rate – the proportion of stolen credentials that are valid. For financial institutions, this rate is often around 10% due to the use of unique credentials and enhanced security practices by users. Based on an average quality list with 1 million credentials, the estimated total number of harvested credentials from an ATO attack is approximately 100,000.



2. Attacker's Reputation: On the dark web, the reputation of the attacker influences the success rate of selling stolen credentials. Highly reputable attackers can sell up to 60% of their inventory, while those with lower reputations may sell only 20%. It's worth noting that attaining a high reputation is particularly challenging in the banking sector.

3. Account Market Price: The price of stolen credentials varies by industry. A bulk sale of banking credentials offers a relatively large potential attacker income of approximately $0.40 per credential, reflecting their value in fraudulent activities.

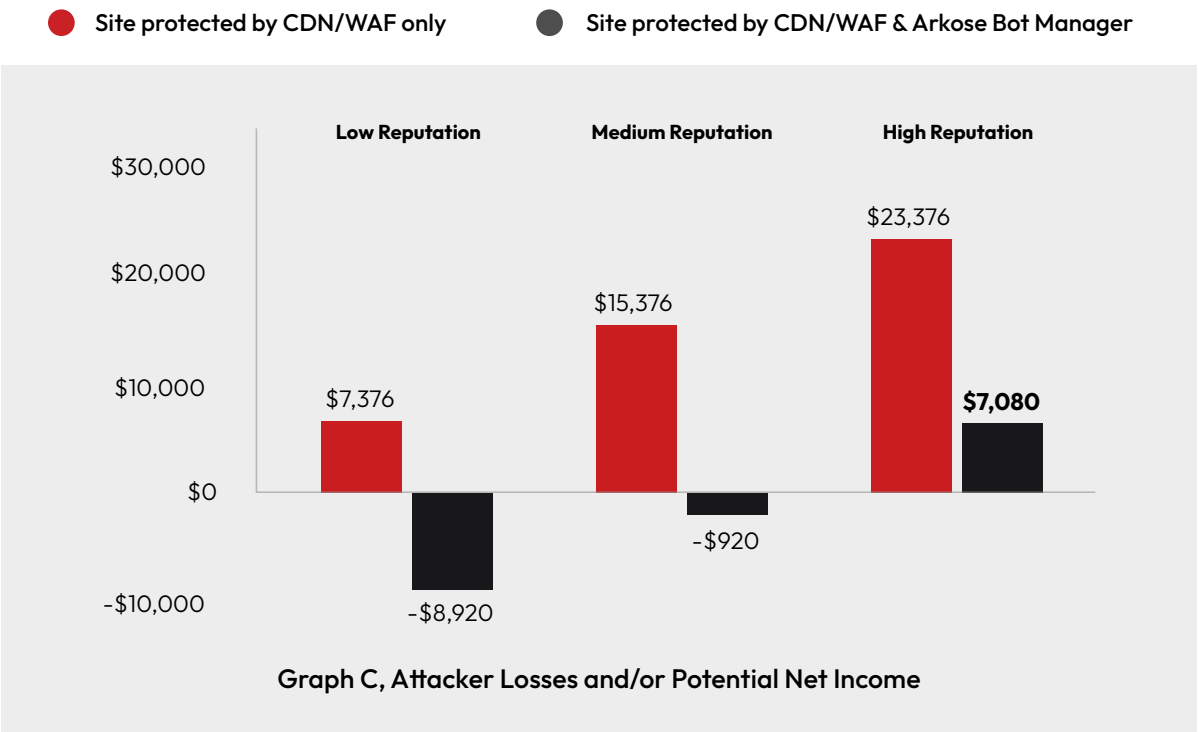
Cost and Impact of Security Measures

This paper compares the economic impact of basic CDN/WAF protection against advanced solutions like CDN/WAF combined with the Arkose Titan solution. Basic CDN/WAF setups provide minimal deterrence, allowing attackers to execute attacks with relatively low costs and high profitability. In contrast, integrating Arkose Titan significantly increases cost and complexity of attacks.

[1]www.meridianlink.com/blog/account-takeover-an-emerging-trend-with-costly-outcomes-for-community-financial-institutions

- **CDN/WAF Only:** Attackers can conduct ATOs with modest expenses, often making it a viable exercise. The cost of attacking a site protected only by CDN/WAF is around $624 annually, with potential profits ranging from $7,000 to $23,000, depending on the attacker's reputation.

- **CDN/WAF & the Arkose Titan solution:** When an advanced solution like Arkose Titan is added to a site's security stack, the attack cost rises substantially. The total annual cost for attackers increases to approximately $16,000, due in large part to the cost of the challenge-solver service, making the site a much less attractive target. This results in negative net income for many attackers, particularly those with lower reputations.



Graph C, Attacker Losses and/or Potential Net Income

Economic Impact of Advanced Protection

Advanced security measures, particularly those combining CDN/WAF with Arkose Titan, undermine the economic viability of ATOs. By increasing the cost and complexity of executing attacks, these measures deter attackers and reduce the profitability of criminal activities. The "better together" approach not only enhances security but also sabotages the attacker's cost-benefit analysis, shifting the landscape in favor of defenders.

This white paper underscores the critical importance of integrating advanced security solutions to counteract the growing threat of ATO attacks. For financial institutions, adopting a comprehensive, layered security strategy is essential to safeguarding assets, maintaining customer trust and mitigating financial losses.

The economic implications outlined here make a compelling case for enhancing your security posture. To discuss how these findings can be tailored to your specific needs, please reach out to us.

The Economics of ATOs in Banking: An Introduction

Cybercriminals profit by exploiting vulnerabilities in systems, applications and human behaviors, often finding lucrative opportunities in account takeover (ATO) attacks. Here at Arkose Labs, we're committed to understanding the profitable business model that fuels cybercrime. This informative white paper takes a deep dive into the economics that drive these online attacks. It particularly focuses on that critical moment when a cyber threat shifts from being a feasible option for an attacker to a losing proposition. That's precisely where the right security solution can make a monumental difference. This white paper will help you understand how your financial services platform can achieve sustainable, cost-effective protection against account takeover attacks in a landscape that's constantly changing. Let's explore these hidden dynamics together as you equip your organization for the challenges ahead.

Account Takeover Overview

For cybercrime operations to make economic sense, the money they bring in needs to outpace the costs involved. One of the most profitable and common types of cyberattack is account takeover (ATO). These complex incidents, including credential stuffing, often involve multiple steps and a mix of automated bots and human trickery.

Understanding the sophistication and profit motive behind ATO attacks sets the stage for grasping their broader impact. Numerous studies and reports carried out over time have consistently demonstrated the widespread danger of ATO fraud, affecting businesses and individuals. According to TransUnion's 2023 State of Omnichannel Fraud Report, account takeover fraud has surged 81% over the previous four years, with many credit unions and community banks experiencing a noticeable rise in such incidents.[2]

This rapid escalation points to the urgent need for individuals and organizations to adopt advanced security technologies and practices to mitigate this threat.

1. **Data is a massive target**. When a company falls victim to a breach, it can result in the violation of customer trust and monumental financial losses. In 2024, the global average cost of a data breach reached an all-time high of $4.88 million, marking a significant 10% increase from the previous year.[3]

2. **Stolen credentials open up even shadier opportunities.** This valuable information is then disseminated on the dark web or public "attack service" platforms.

3. **Cybercriminals exploit this data to launch other attacks.** Consumers often employ the same logins and passwords across multiple platforms, which means bad actors can easily engage in ATO attacks. Hackers systematically test stolen credentials against various potential targets, often generating a refined list of valid accounts across different websites.

4. **Attackers profit by selling these packages.** The resulting inventory of confirmed accounts, typically sold in bundles of 100 to 1,000 accounts on the dark web, varies in price by industry. Attackers specializing in ATOs acquire these credentials and use specific monetization techniques tailored to the targeted websites. This work is often done manually and not in massive volumes once the accounts are validated.

[2]www.meridianlink.com/blog/account-takeover-an-emerging-trend-with-costly-outcomes-for-community-financial-institutions
[3]newsroom.ibm.com/2024-07-30-ibm-report-escalating-data-breach-disruption-pushes-costs-to-new-highs

Research Approach and Assumptions

This research aims to investigate the methods used by attackers who specialize in account takeover attacks on banking institutions, comparing the effectiveness of sites protected by a content delivery network (CDN)/basic web application firewall (WAF) versus those secured by a CDN/WAF plus an advanced solution like Arkose Titan, underscoring the value of a "better together" strategic mindset in cybersecurity. The study analyzes the infrastructure and tools attackers must deploy to penetrate each type of defense. Ultimately, we'll determine how effective adding an advanced bot detection and mitigation solution to your tech stack is in eroding the economic incentive of today's attackers.

This white paper relies on data gathered from the dark web, Telegram, Discord and other social media platforms, along with insights from the Arkose Global Intelligence Network. We made reasonable assumptions regarding the attacker's potential income from cyberattacks, considering their reputation and the likelihood of inventory sales.

How Criminals Exploit Weak Security

When a bank's site is poorly protected, criminals don't need to worry about deploying a complex infrastructure for credential stuffing attacks. Instead, they can easily employ a botnet with a limited number of nodes, using off-the-shelf tools. The main concern is throttling the request flow to avoid overwhelming the target website. Sometimes, this poorly calibrated attack may unintentionally lead to denial of service and prolong the verification process for a large set of credentials.

In this simplified scenario, the botnet could consist of just one machine, such as a laptop running a Sentry MBA script, complemented with tools like STORM to manage CAPTCHA solving, and distributing requests through cheap proxies in data centers. It's worth remembering that this uncomplicated setup can bypass basic CDN/WAF settings.

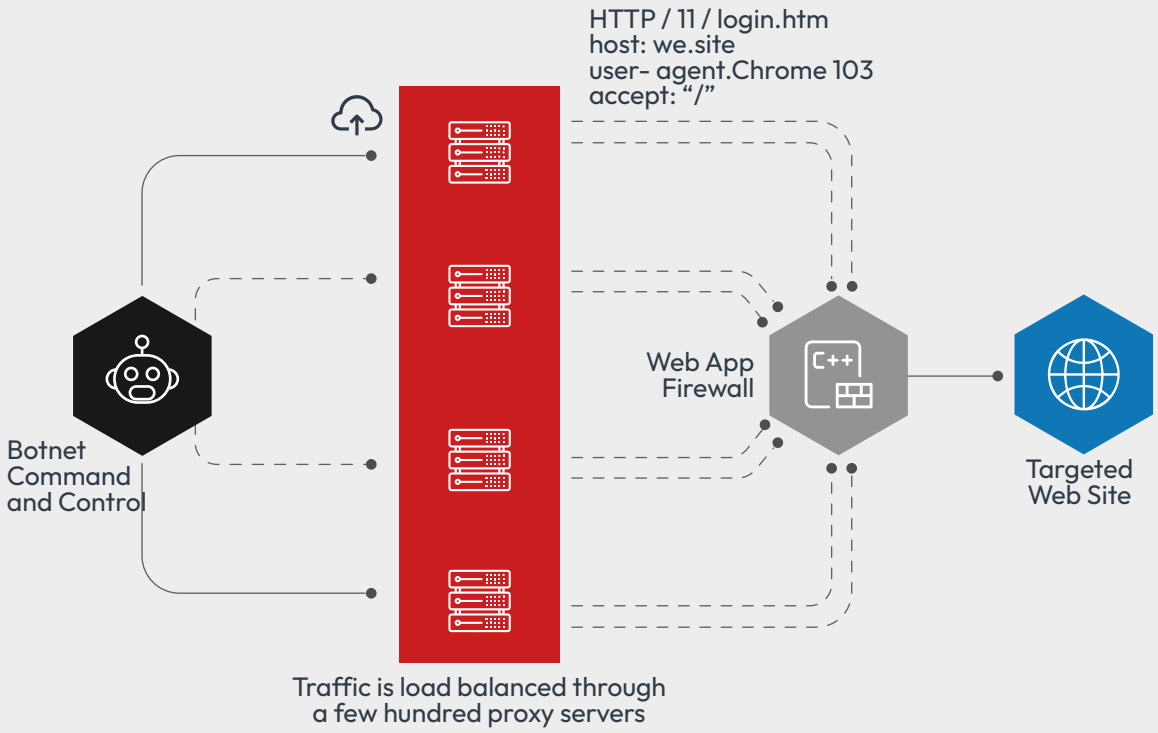


Diagram 1: Example of simple automated attack.

With the capabilities of advanced bot detection and mitigation systems in place, attackers need increased sophistication to evade detection. Attackers are updating their strategies to include additional resources such as:

- Spreading traffic through a vast botnet of over 10,000 nodes across multiple continents
- Masking the traffic's origin to appear as residential and mobile ISPs rather than data centers to avoid suspicion
- Mimicking legitimate user behavior, following similar workflows to access resources
- Sending expected data and ensuring variety in the fingerprint to avoid detection based on client-side characteristics
- Dealing with a significant portion of the attack traffic being blocked or challenged, necessitating resubmissions and lengthening the attack process

The infrastructure for such attacks may involve a laptop orchestrating virtual machines in a cloud infrastructure, generating traffic through residential and mobile proxies. The software used can range from advanced Python scripts to headless browsers that mimic complex user behaviors. Additionally, the botnet must employ CAPTCHA-solver services—using AI or low-cost human workers—to overcome challenges.

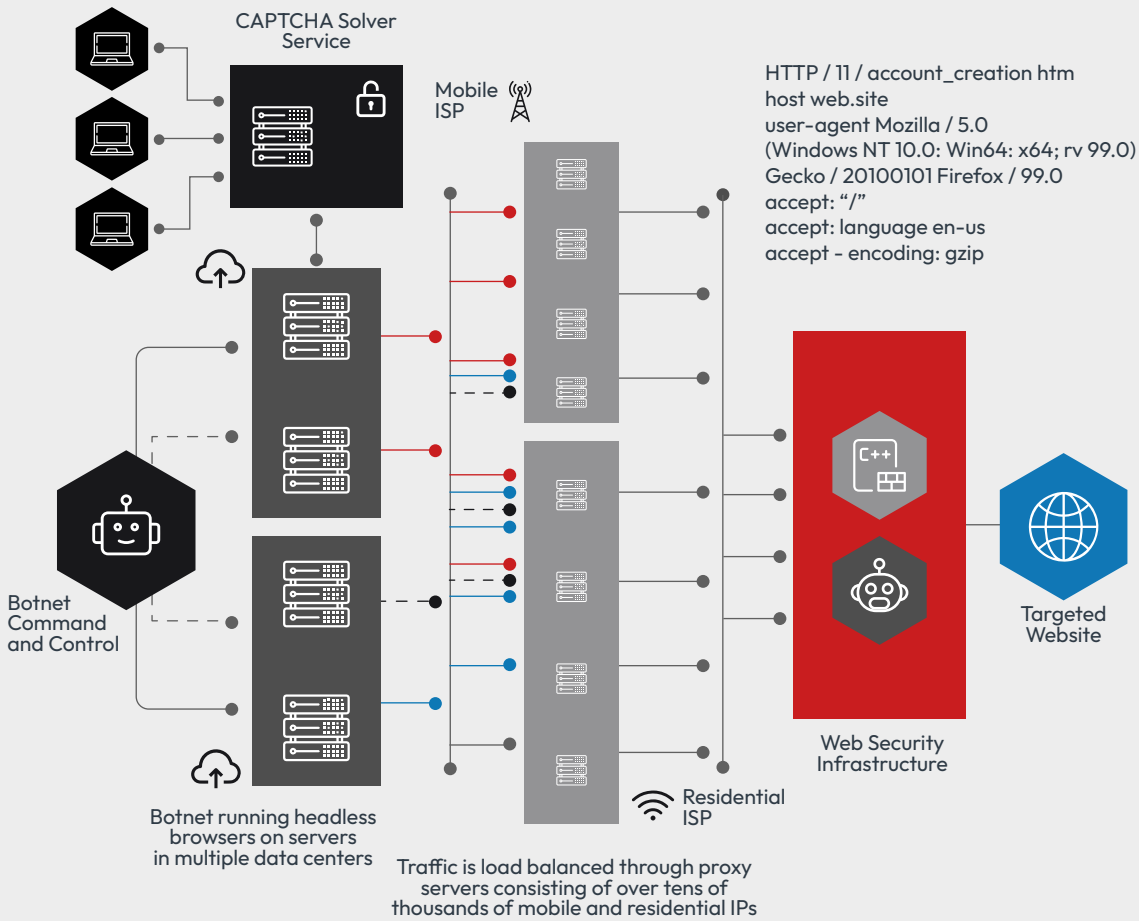


Diagram 2, Deployment with Arkose Titan

Factors Affecting an Attack's Revenue Potential

Before digging into the cost, let's evaluate the factors that will affect the revenue potential for attackers.

Hit Rate

This metric determines the number of valid sets of credentials harvested from the ATO attack. The ratio can vary based on the industry and the quality of the list, which contains known username and password combinations.

Financial services' websites often don't use email addresses as user IDs, which affects the hit rate. Consumers are also more cautious about reusing credentials from other sites for their bank login. As a result, an expected hit rate of 10% is anticipated.

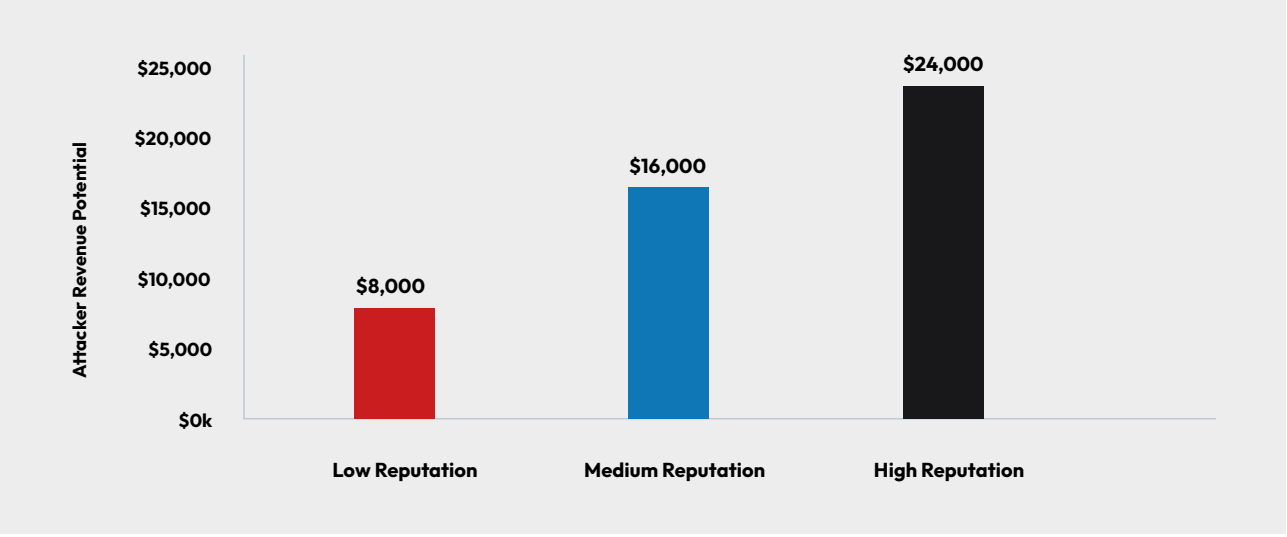
Based on an average quality list with 1 million credentials, the estimated total number of harvested credentials from an ATO attack is approximately 100,000.

Attacker's Reputation

The dark web serves as a marketplace for legitimate and fraudulent goods and services. Criminals exploit these platforms to sell private information obtained from account takeovers. A reseller's reputation directly influences the percentage of their inventory that gets acquired. New resellers with no or low reputation may sell up to 20% of their inventory, medium-reputation resellers may sell up to 40%, and highly reputable resellers may sell at least 60% of their inventory.

Account Market Price

The market price of a user's credential varies by industry, with a bulk sale of banking credentials offering a relatively large potential income of approximately $0.40 per credential. Graph A shows the current market price and potential revenue based on the estimated credentials harvested after completing an attack.



Graph A, Attacker Revenue Potential Based on Attacker Reputation (Percent of Inventory Sold)

Performance of the Web Security Product and Team Protecting a Site

The more protected the site, the more likely it will be that the least patient or least skilled attacker will give up their attack before it completes – and move on to an easier target. More effective security products are likely to stop or challenge close to 100% of attack traffic, increasing the need for the attacker to resubmit requests. This move extends the timeline to completion and, in many cases, the cost of the attack.

Frequent software updates are essential for adjusting the botnet's attack strategy to overcome existing defenses. Certain updates may require extensive testing and development, spanning days or weeks. Some attackers may ultimately abandon their attack if they can't overcome the defense in place. Defenders and attackers feel the pressure to stay vigilant. Table A shows the estimated time for completing an account takeover attack with one million credentials, considering attack velocity and assuming no downtime due to software updates necessitated by a strong defense strategy protecting user identities.

Humans can be impatient and often prefer to execute attacks quickly by sending requests at a high velocity. However, this approach has drawbacks for the bad actors. It makes the attack more noticeable to defenders and increases the total number of requests needed to succeed. For sites protected with solely a web application firewall or content delivery network, attackers are better off adopting a low attack velocity to stay unnoticed and minimize the number of replays required. By doing so, the attack can be completed within approximately two and a half days.

Attack Velocity	Requests / hour	Replay Factor	Total Requests	Est. days to complete
Low	25,000	1.5	1,500,000	2.50
Medium	50,000	3	3,000,000	2.50
High	150,000	6	6,000,000	1.67

Table A, Time to Complete Account Takeover with 1 Million Credentials, CDN/WAF Only

For well-protected sites, however—those protected by a CDN/WAF plus a bot detection and mitigation solution like Arkose Bot Manager, a core component of Arkose Titan—the challenge strategy effectively hinders attack speed. This is achieved by countering traditional CAPTCHA-solver services, which often have limited staffing capacity. If, for instance, a CAPTCHA-solver worker can handle three CAPTCHAs per minute and about 100 workers are assigned to solve the attack's challenges, the attackers can achieve a maximum request rate of 18,000 requests per hour. However, this approach also amplifies the replay factor, considering potential solver errors and time constraints. Consequently, the attack completion time may more than triple, as seen in Table B.

Requests / hour	Replay Factor	Total Requests	Est. days to complete
18,000	4	4,000,000	9.26

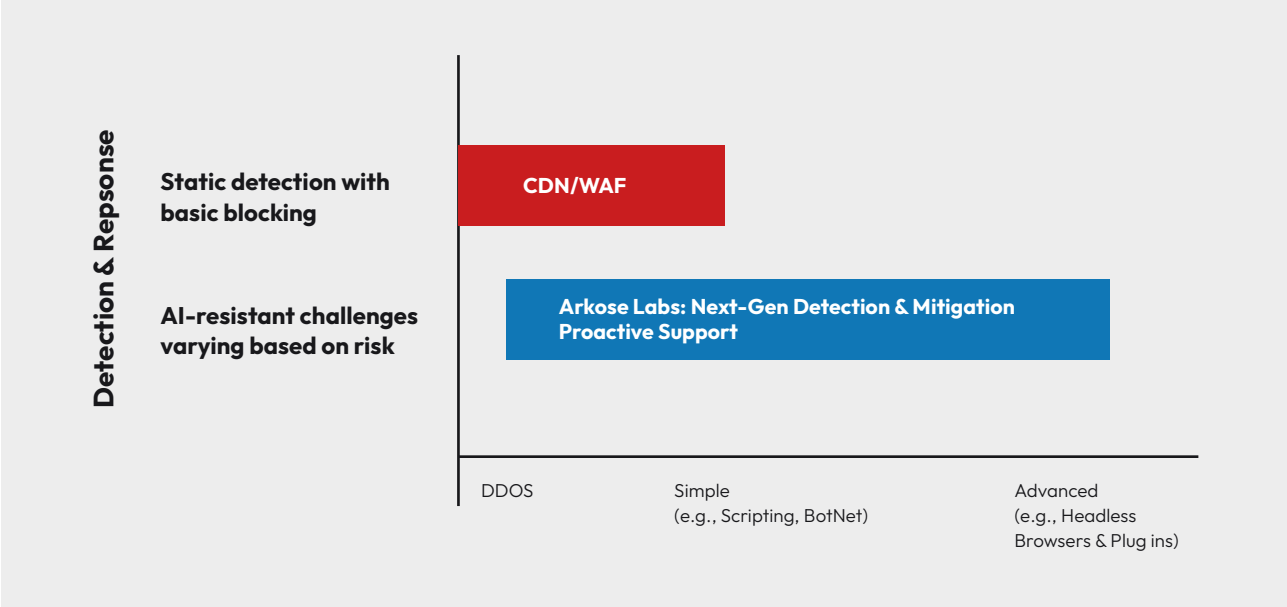
Table B, Time to Complete Account Takeover with 1 Million Credentials, CDN/WAF & Arkose Bot Manager

When attacking a well-protected site, the number of replays, the lack of fast progress, the complexity of the attack strategy, the rising cost and the uncertainty of how long the attack will take to complete may deter attackers and convince them to give up early, significantly affecting their inventory and ultimately sabotaging their net income.

Better Together: How Advanced Protection Strengthens the Tech Stack

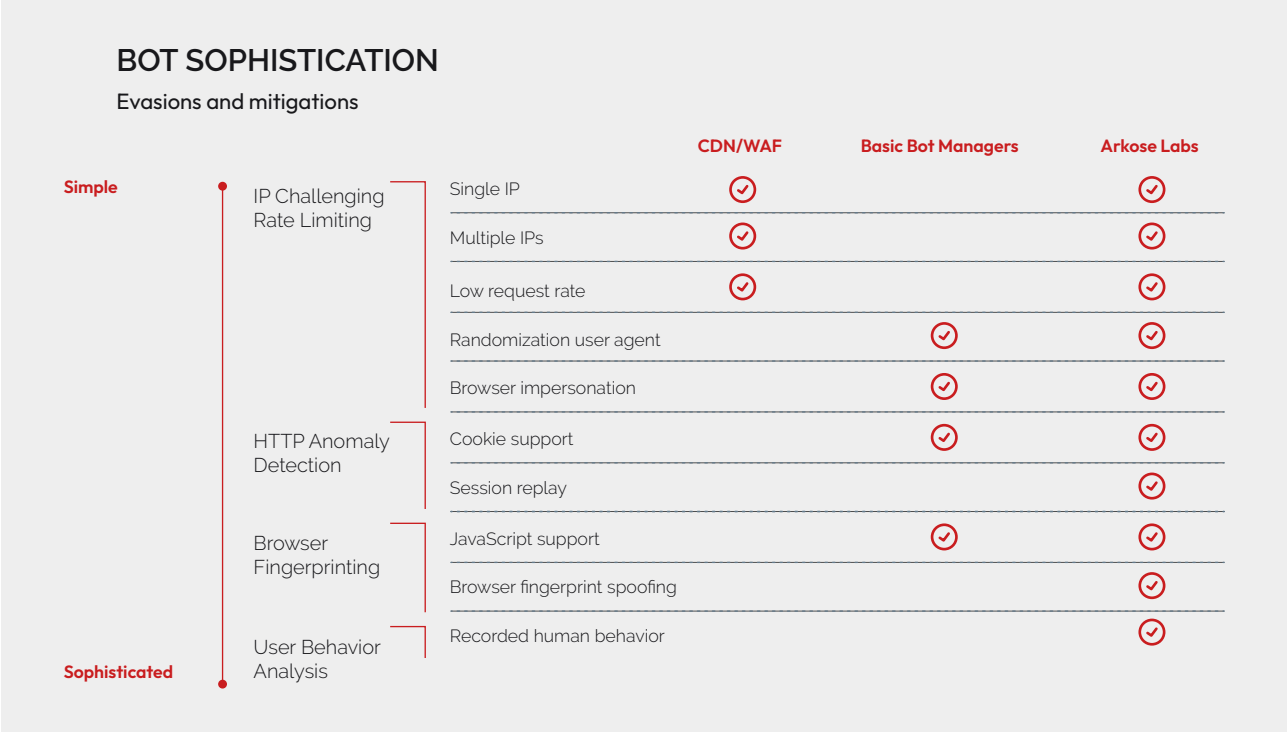
A layered cybersecurity solution stack, including a web application firewall or content delivery network to stop DDoS attacks and block bots at the edge, is crucial for defending against common application layer threats. Each solution in the stack is purpose-built and excels in its area of expertise. However, CDN/WAFs, while providing some bot detection capabilities, may not effectively handle more sophisticated and persistent attacks like AI-powered account takeovers (ATOs). Despite these layers, malicious bot traffic can still slip through the cracks.

To achieve comprehensive security, integrating an advanced bot management solution is crucial. Arkose Titan enhances your cybersecurity posture by employing advanced decisioning, threat intelligence and adaptive defenses tailored to counteract sophisticated bot-driven threats. This ensures that only legitimate users gain access to critical resources, effectively closing gaps that traditional CDN/WAF solutions might miss.



Arkose Titan complements existing WAF and CDN solutions by offering real-time feedback and adaptive challenge mechanisms. This approach significantly reduces false positives and enhances overall security effectiveness. With Arkose Labs, your defenses evolve in tandem with attack sophistication, ensuring that your cybersecurity measures remain ahead of emerging threats.

When attacking a well-protected site, the number of replays, the lack of fast progress, the complexity of the attack strategy, the rising cost and the uncertainty of how long the attack will take to complete may deter attackers and convince them to give up early, significantly affecting their inventory and ultimately sabotaging their net income.



Costs to Attack a Website

Attacking a Site Protected With a Content Delivery Network/Web Application Firewall

The infrastructure needed for a successful attack varies based on the protection a company has in place. A website protected with a CDN/WAF solution only, as seen in Table C, will require a basic shared data center-hosted proxy service to defeat the rate limiting in place. The average cost for such service at the time of this writing is $52 per month.

Proxy cost (monthly)	$52
Total cost (monthly)	$52
Total cost (yearly)	$624

Table C, Cost to Attack a Site Protected by CDN/WAF Only

Attacking a Site Protected With a CDN/WAF and Arkose Titan

Websites protected with an advanced bot management solution that includes dynamic challenge capabilities like those of Arkose Bot Manager will require attackers to double the hosting cost per site they attack to manage the more complex workflow of solving the challenge. It will additionally require the attacker to integrate the botnet with a challenge-solving service. The average cost at this time is $1.83 per 1,000 requests.

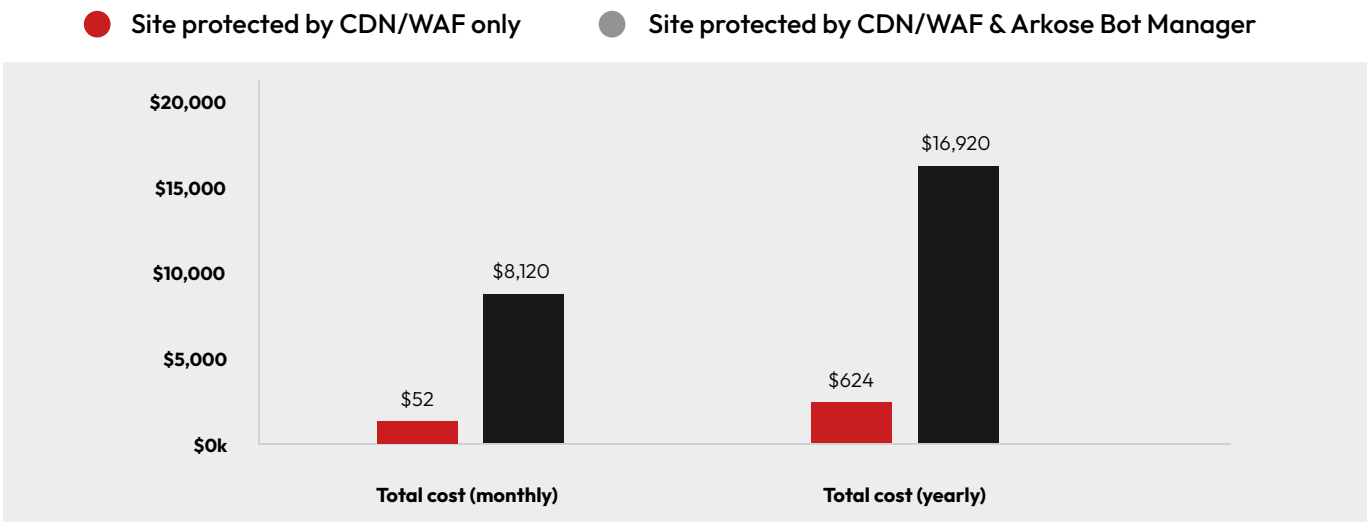
The limited bandwidth will substantially extend the time required to complete the ATO, making it more noticeable and giving the defender ample opportunities to intervene, thereby increasing the number of retries needed.
For this simulation, let's consider that a credential needs to be submitted to the challenge-solving service four times before it is successfully validated. In this case, it will require about 4 million requests to validate 1 million credentials. Table D summarizes the total cost.

CAPTCHA solver cost (one-time)	$7,320
Hosting and storage cost (monthly)	$100
Proxy cost (monthly)	$700
Total cost (monthly)	$8,120
Total cost (yearly)	$16,920

Table D, Cost to Attack a Site Protected by CDN/WAF & Arkose Bot Manager

It's worth noting that many CAPTCHA solvers will not even attempt to tackle Arkose Bot Manager's AI-resistant challenges. The time it takes to solve them is too costly for attackers, and the effort cannot be effectively automated.

Here's a side-by-side comparison, as seen in Graph B:



Graph B, Cost to Attack a Site, Differing Protection Levels

The Attacker's Net Income

Now that we have a good understanding of the potential revenue and cost of attacking a website, let's see how the business of cybercrime is affected by these two different levels of cybersecurity protection.

Net Income Against a Site Protected With CDN/WAF Only
Let's first consider a site protected with a CDN/WAF solution with some basic bot management rules and rate imiting. As you can see in Table E, an attacker can make some money from Day One even if they are starting with

no experience. Considering the low level of skill, infrastructure and maintenance required to carry out the attack, it may be done as a hobby or even a side hustle for additional income. This may potentially attract a lot of “script kiddies" who are looking to make a few bucks.

Total cost (yearly)	$624
Attacker income	
Low reputation	$7,376
Medium reputation	$15,376
High reputation	$23,376

Table E, Attacker Net Income Against a Site Protected With CDN/WAF Only

Attacker Net Income Against a Site Protected With CDN/WAF & Arkose Titan

Now, let’s consider the possible net income for sites protected with both a CDN/WAF and the Arkose Labs solution, which includes bot detection and mitigation—and the most advanced challenge-response mechanism on the market. What makes a huge difference here is the cost of the challenge-solver service that is required, which, considering the volume of requests needed to complete the attack, can go into the tens of thousands of dollars.

Table F illustrates how attackers with low and medium reputations incur losses. The landscape may initially seem somewhat favorable when focusing on seasoned attackers with strong reputations. However, the rise of cybercrime-as-a-service (CaaS) has lowered the entry barrier, leading to a surge in less experienced attackers. These individuals often lack advanced skills and heavily rely on widely available CaaS tools. Within the cybercriminal community, they are typically seen as less capable and more dependent on the efforts of others, which affects their reputation.

Total cost (yearly)	$16,920
Attacker income	
Low reputation	-$8,920
Medium reputation	-$920
High reputation	$7,080

Table F, Attacker Net Income Against a Site Protected With CDN/WAF & Arkose Bot Manager

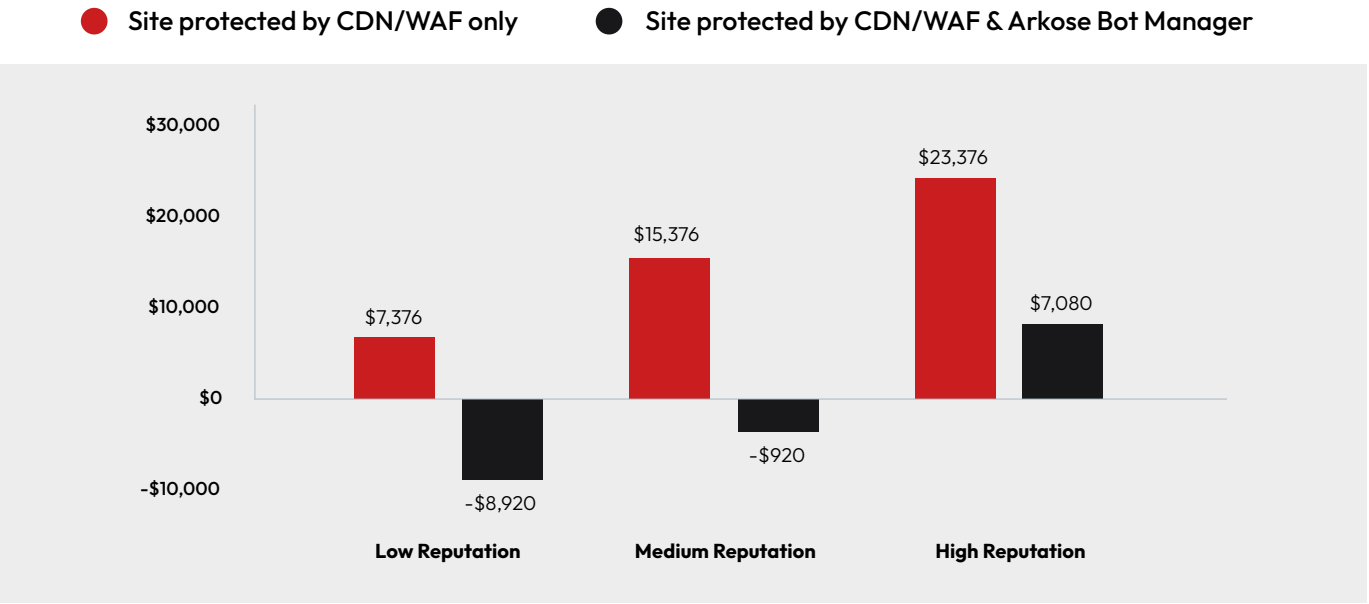
The Economic Impact of Advanced Security Measures

The profitability of account takeover attacks is directly influenced by the effectiveness of the security measures protecting a site. When comparing sites protected by a CDN/WAF alone to those fortified with both a CDN/WAF and the Arkose Labs solution, the economic incentives for attackers shift dramatically.

Sites protected by a CDN/WAF alone offer a relatively low-cost opportunity for attackers, making them attractive targets. Even novice cybercriminals can profit with minimal investment, leading to the proliferation of such attacks. The low cost of conducting these attacks and the potential for substantial profits, especially for attackers with a high reputation, makes these sites prime targets.

Sites protected by both a CDN/WAF and Arkose Titan, however, present a much more challenging and costly endeavor for attackers. The additional layers of bot detection, dynamic challenges and advanced threat mitigation significantly increase the complexity and cost of executing a successful ATO attack. As the cost of the attack rises, the profitability diminishes, often leading to negative returns, especially for less experienced attackers.

Graph C illustrates the stark contrast in losses/potential income for attackers when attacking a site with different levels of protection.



Graph C, Attacker Losses and/or Potential Net Income, Different Protection Levels

As shown in Graph C, attackers targeting sites with only a CDN/WAF can expect substantial net income. In contrast, attackers going after sites protected by a CDN/WAF and Arkose Titan face significantly higher costs, often leading to losses unless they have a very high reputation and can successfully resell their inventory at premium prices—a feat that is typically challenging in the banking sector. This makes it less feasible for attackers to sustain their operations in the long term.

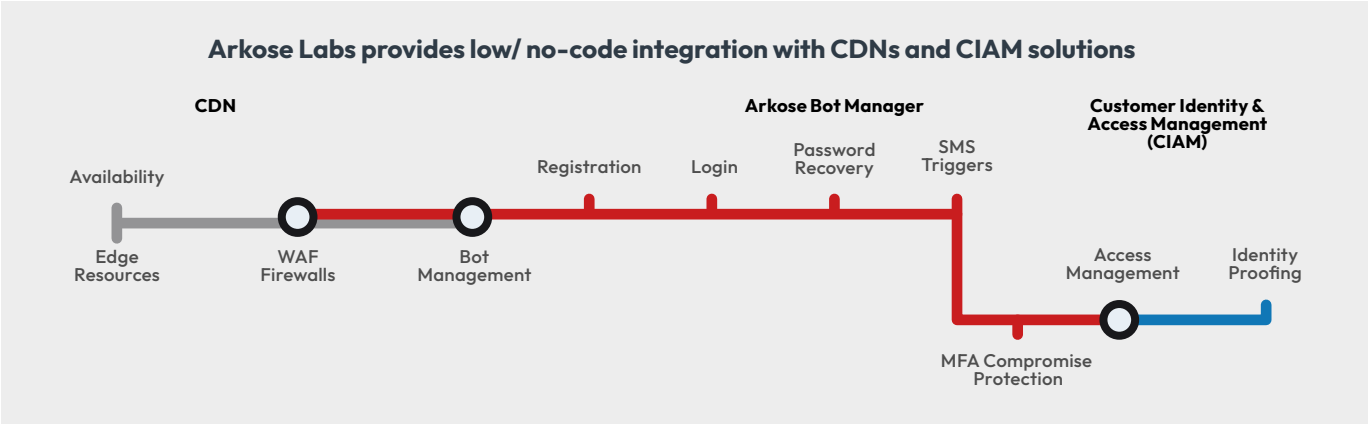
Conclusion

The motivating intention of this paper is to reveal the economics behind one of the most lucrative types of online attacks fraudsters perpetrate: ATOs. This is a worthy endeavor because for a financial services enterprise to reduce cyberattacks and internal security costs, it is critical first to understand the underlying economics. After deep research and analysis, this white paper clearly outlines how ATOs happen, the factors that influence whether an attack will generate net income for a cybercriminal, and how various types of defenses drive up the attacker's cost.

Experienced attackers with strong reputations on the dark web can still make decent revenue, while new entrants struggle to start and earn enough. When comparing different levels of web security solutions, however, some defenses significantly raise the attackers' costs and sabotage their potential earnings. This encourages attackers to either halt their activities or target less protected entities.

Additionally, this paper sheds light on a crucial aspect of ATO: the time-factor for an attack. It answers the question of how long an attack will take, based on a company's defense controls. If the attack is too time-consuming, it often prompts the attacker to give up and move on to easier targets.

The strategic "better together" integration of Arkose Titan alongside a CDN/WAF dramatically reduces the profitability of ATO attacks. While traditional tools help you to detect and mitigate simple bots, by adding Arkose Titan to your security stack, you'll get a managed service experience with dedicated experts who have industry-specific knowledge and a proactive approach. This gives you a robust defense-in-depth strategy, leading to significant cost savings and enhanced security. We make it easy to deploy this "better together" risk mitigation stack by offering a low-code integration and easy set-up.



For financial institutions and other organizations, this means not only a reduction in successful attacks but also a deterrent effect. In a world where the economics of cybercrime are a motivating factor, this defense-in-depth approach to security turns the tide against attackers, protecting your customers and your bottom line.

BOOK A DEMO

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.