Arkose Labs

Protecting Technology Platforms From Fraud Attacks

Keeping the Global Digital Economy Safe

Ebook

Tech Platforms Power the Global Economy

Cloud-based tech platforms are a critical part of the global digital economy. They connect people from around the world and allow them to collaborate, share files, and work in an efficient and centralized manner. With millions of users on these platforms, there's no surprise that fraudsters flock to them as well. The recent worldwide lockdowns related to the COVID-19 pandemic, and the way societies are now operating even as the world slowly returns to normal, have shown how critical it is to have platforms in place that can efficiently connect people from around the globe. The world is becoming ever more digital, and cloud-based platforms are the glue that holds this new reality together.

Tech platforms can be incredibly useful, cost-effective tools for businesses that not only make their lives easier but also provide cost savings and a better ROI. Over the past decade, with the rise of smart devices and the "app economy," companies have had to adjust their technology strategies to ensure their customer experience is as intuitive, seamless, and user-friendly as possible. This shift has enabled businesses to leverage technology to save money, increase their ROI, and provide better customer service.

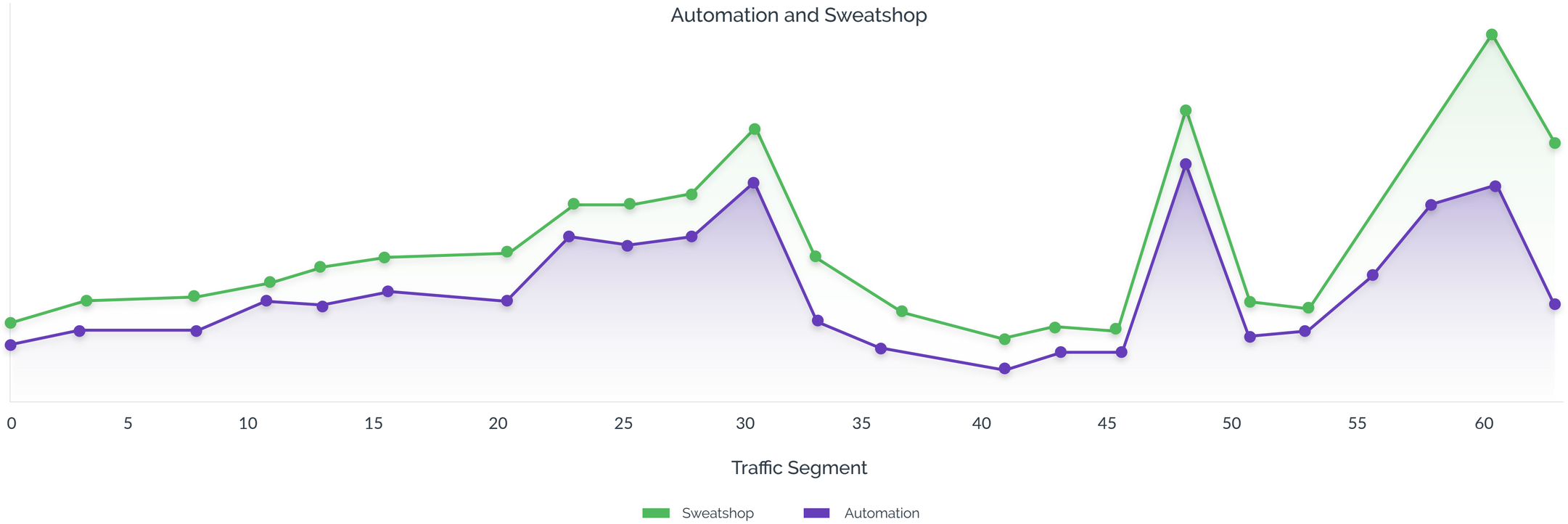
An Interconnected Consumer Experience

This means cloud-based tech platforms must balance a seamless user experience with robust fraud controls. This can be a difficult line to toe. Leaning too far in one direction or the other can result in too many false positives, or too many attackers getting through. But securing B2B and B2C tech platforms is paramount. More than ever before, these platforms connect most every aspect of our digital lives, and in many ways power the global digital economy.

Changing Digital Habits

The COVID-19 pandemic changed many of the ways people work and interact with each other. Though the world is now regaining a sense of normalcy and most lockdown orders have been lifted, many of the digital habits that were started during the pandemic will likely continue on.

That means businesses of all stripes must be prepared for a permanent increase in digital traffic. The shift towards digital is not an anomaly that will revert back after the pandemic ends. Rather, it actually represents a new phase in the history of the internet, one where more people than ever before became comfortable conducting much of life's business in the digital realm.



Here are some of the ways COVID-19 has permanently altered digital habits and increased the use of cloud-based platforms in everyday life.

Working:

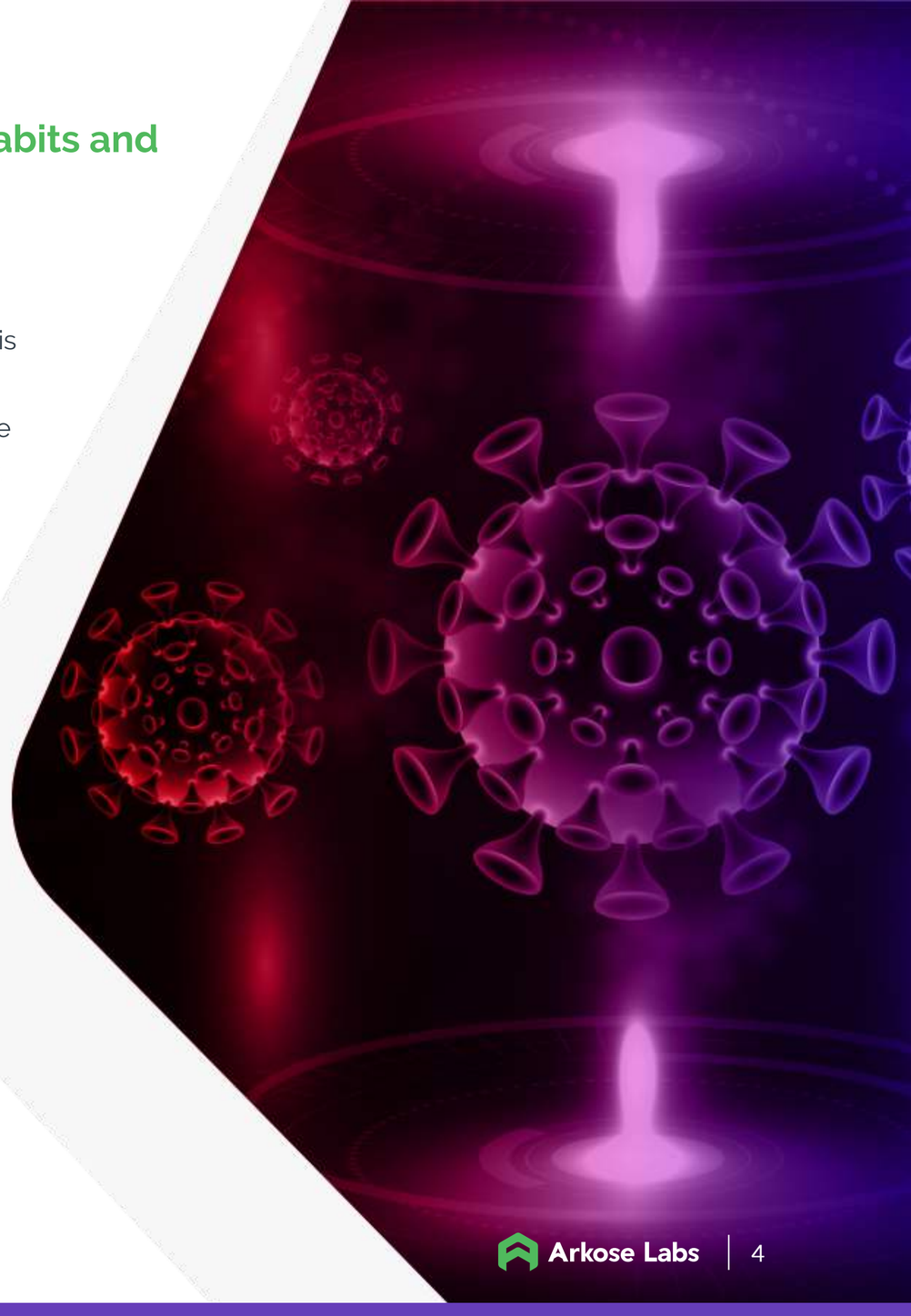
It will likely be years before offices are filled to capacity and operating as they did pre- Covid. This is due not only to health reasons, but also many businesses that had previously not considered the viability of remote working are now changing their minds. As companies see they can get the same productivity as before, while reducing overhead costs such as office space, platforms that enable remote work and collaboration will only continue to be more valuable.

School

Any parent during the pandemic became acquainted with the pros and cons of “remote learning.” While schools are gearing up to reopen, this style of learning will likely continue in some capacity, such as with extracurricular activities like music lessons or language lessons.

Social Gatherings:

As we’ve seen with the reopening of restaurants and outdoor gatherings, people won’t be having “Zoom happy hours” forever. But some social events could remain in a virtual setting for the foreseeable future. Perhaps grandma’s 80th birthday party might be held on a digital platform, rather than in person. Furthermore, friends and relatives in disparate areas may start to have more virtual get-togethers, now that people are more used to the idea of doing so.



Different Types of Fraud Attacks Targeting Tech Platforms

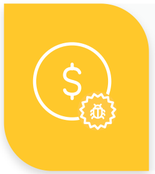
As noted, this rise in traffic to digital platforms has also attracted a rise in fraudsters to them. Attackers have several different ways to monetize attacks on cloud-based platforms. Here are just a few:

ATO Attacks:
These attacks aim to steal valuable user data, which can include things like payments information or PII. They are also used for account remuneration, whereby fraudsters attempt to verify whether a certain user account exists or not.

New Account Fraud:
Technology platforms are a prime target for fraudsters looking to abuse free trials and set up new accounts using stolen or synthesized credentials.

Scraping:
Also using bots, attackers can scrape large amounts of publicly available information from platforms. This can be used to resell to third parties, or other criminal purposes.

Phishing:
Wherein new accounts are created at scale, and then used to send malicious messages to other users of the platform, such as to try and get them to download a dangerous link or to disseminate spam.



Bonus Abuse:
Fraudsters deploy bots at scale to create new accounts in order to abuse promotional offers meant to attract new customers, such as free storage space or server time. This hinders customer acquisition efforts and defrauds good new users whom the promotions were meant for.

Increased Fraud Attacks Strain Resources

Dealing with the issue of increased traffic and online fraud can be a major challenge for businesses and can put a strain on internal resources. By investing in tech solutions to help manage the traffic and fraud, your company can significantly reduce costs and increase ROI. This investment also helps to ensure that customers have a smooth and secure user experience while your internal fraud and security teams can remain vigilant in protecting customers and the platform.

Shift the attack surface in order to operate more efficiently.

Using a third-party solution as your first layer of defense against fraud can potentially lead to significant cost savings and better ROI. Not only does this shift the attack surface so attackers target a third party instead of your business, but it also frees up internal teams to operate much more effectively, allowing them to fight fraud and abuse in a much more efficient manner.

The Ideal Way to Identify and Segment Traffic

By properly assessing the threat level of each user and classifying traffic based on intent, tech platforms can accurately identify and combat fraud while saving costs and increasing their ROI without impacting the customer experience. This ensures that good customers are not blocked and suspicious traffic can be quickly and efficiently triaged and challenged.

A Two-Pronged Approach

Such a third-party solution should have two main components: Robust detection and analysis in order to properly identify traffic, and an effective enforcement challenge that stops bad guys at the front door while not impacting good users who may see it.

Detection:
All data from user sessions should be analyzed in real-time to help recognize the context, behavior, and past reputation of every request. Continuously evolving detection methods using probabilistic, statistical and machine learning-based models to detect patterns ensure that your business is protected now and against evolving threats in the future.

Enforcement:
After analysis, traffic is then triaged, with suspicious users facing a challenge. The challenges need to be able to stop even the most advanced bot machine vision technology. Human fraudsters, meanwhile, are fed increasingly complex challenges that waste their time and effort, so that they eventually give up and attack another site that isn't yours.

The Arkose Labs Approach

Arkose Labs prevents all forms of fraud and abuse targeting tech platforms:

Account Takeover

New Account Fraud

Scraping

Credential Stuffing

Bonus Abuse

The Arkose Labs platform was designed from the outset with user experience in mind. Difficult or faulty authentication experiences can be very damaging to brand value and the bottom line. That's why the platform blocks no traffic, but rather serves suspicious traffic with targeted enforcement challenges.

Arkose Labs can take this approach with confidence due to the high degree of accuracy the platform has in detecting suspicious traffic, and then segmenting good from bad. The platform analyzes a variety of behavioral biometrics and device heuristics in real time, and data fed back from the enforcement challenge creates a feedback loop. This means the platform is constantly evolving in its detection capability. In the small chance a good user sees the challenge, they are not only easy (with an average solve time of less than 3 seconds), but they are also fun to complete and brand-specific as well. Cost savings are realized due to the improved ROI as fewer valid customers are challenged, resulting in a better customer experience and fewer lost sales.

Case Study | Outlook.com

Arkose Labs Helps Microsoft Outlook.com Eliminate Bot-powered Attacks

Outlook.com needed a new way to stop fraudulent new account creations and reduce abuse, while improving customer experience—all in a cost effective manner. This was important not only to protect their own users but to create a safer environment for the wider ecosystem.

Business Problem

- Large-scale fake account registrations.
- Email accounts used for malicious and fraudulent purposes
- Fraud mitigation disrupted good user experience
- Costs associated with manual review processes
- Financial savings from automated processes

Solutions

- Unified authentication for new users
- Innovative challenges to stop bots and fraudsters
- Malicious emails detected and challenged downstream
- Reduced costs associated with manual reviews and fraud prevention efforts

Results

- 33% improvement in good customer throughput
- 98% reduction in fraud and abuse
- Stopped customer complaints about SMS verification

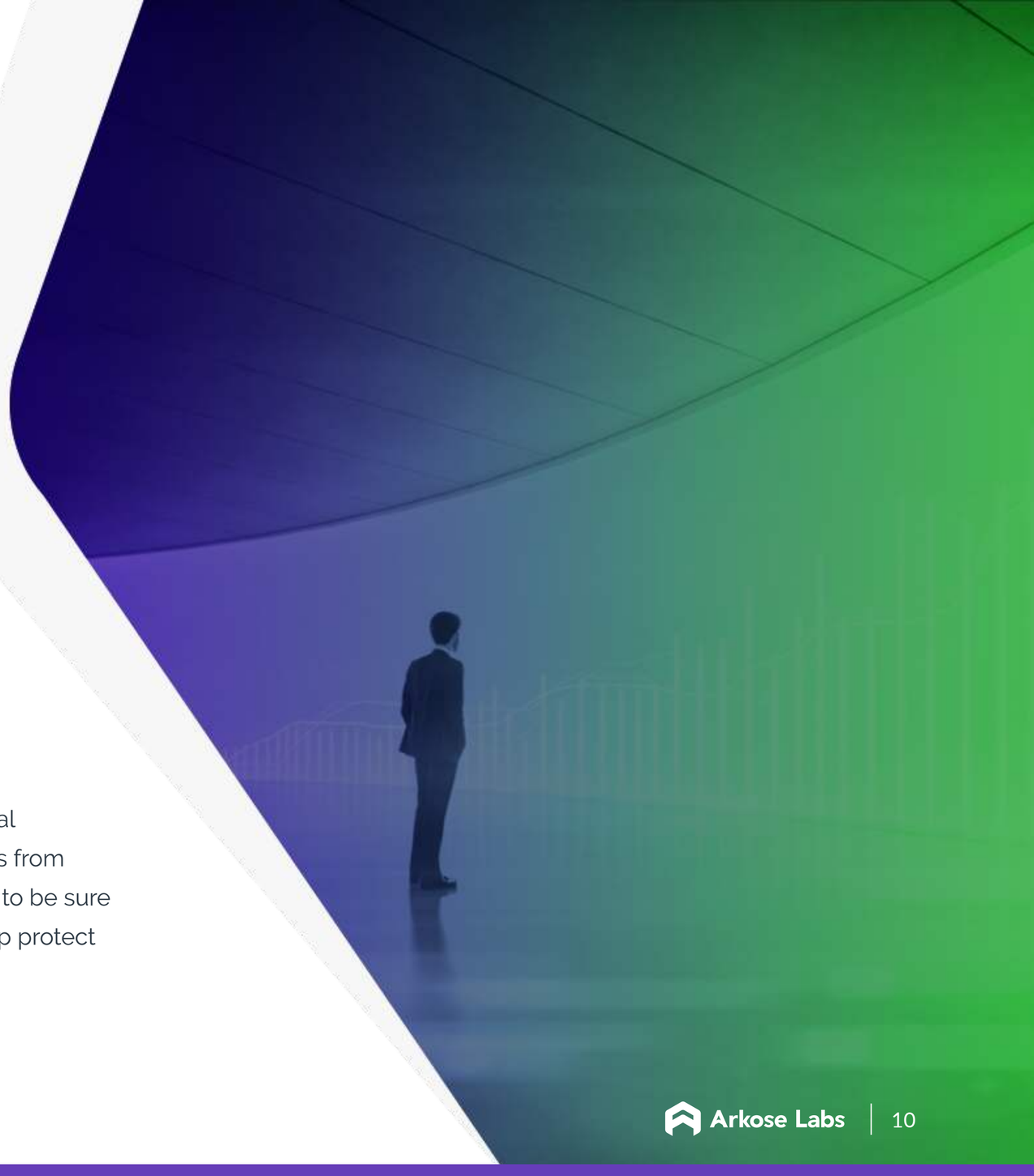
Conclusion

Tech platforms are vital components connecting both consumers and businesses to the digital world. Securing them from fraudsters and keeping users safe is of critical importance, and this will only be more essential as more and more users flock to these platforms and they become even more popular.

This means tech platforms must grapple with strained resources as they serve a greater number of users while also trying to combat fraud. These businesses and consumers have high expectations—the customer experience can't be impacted in the course of fighting fraud.

It's no surprise then that there was an uptick in fraud activity targeting this industry in Q2. Fraudsters used the increased traffic flocking to these platforms in an attempt to blend in with good customers and carry out attacks.

Cloud-based technology offers significant cost savings and a better ROI than traditional solutions. It also provides superior security, safeguarding your business and customers from potential fraud attacks. With more people online than ever before, however, you need to be sure that your data and information is secure. Investing in the right technology now can help protect your business both now and in the future.



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.

Offices

San Francisco
250 Montgomery St 10th Floor,
San Francisco, CA 94104, USA

Brisbane
315 Brunswick St, Brisbane,
Queensland AU

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

Schedule Demo