Google Cloud

Executive Summary:

A defender's guide to mitigating account takeover and bot-driven fraud

Technological innovation: Enabling better digital experiences – and better fraud tactics

There's an insidious, parasitic relationship between innovation and cyber risk: The same technologies that power new and better digital transactions also provide the tools for malicious actors to compromise those transactions. Automation, artificial intelligence (AI), and machine learning (ML) are opening new frontiers for cybercriminals. Account takeover (ATO) attacks are growing by as much as 90% year over year,[1] now affecting half of all businesses[2] and one in four consumers.[3] And AI-powered bots have become essential tools in ATO attacks: Forrester reported that 71% of companies have seen an increase in successful bot-based attacks since the start of the pandemic, and two in three companies report an increase in revenue losses due to these bot attacks.[4]

The cascading impacts of ATO and bot fraud

- **Operational disruption and inefficiency:** Large fraudulent purchases can throw off inventory, as well as supply chain forecasting models and marketing campaigns, using inputs from fraudulent behaviors rather than those of real customers.
- **Revenue and profit loss:** A recent study found half (48%) of enterprises have experienced measurable revenue losses due to ATOs.[5] Estimates quantify typical fraud-related losses at 5% of annual gross revenues. But the reality is that, for roughly half of companies, that figure may be much higher.[6]
- **Damage to trust and reputation:** A substantial part of hidden revenue drain comes from lost customer trust. Two-thirds (65%) of customers will stop buying from a business if their account or credentials are compromised; nearly half will go directly to a competitor; and a third will proactively warn friends to avoid the business.[7] These snowballing reputational effects are long-lasting, painful, and extremely difficult to manage.

[1] https://javelinstrategy.com/2022-Identity-fraud-scams-report
[2] https://services.google.com/fh/files/misc/google_forrester_bot_management_tlp_post_production_final.pdf
[3] https://seon.io/resources/statistics-account-takeover-fraud/
[4] https://services.google.com/fh/files/misc/google_forrester_bot_management_tlp_post_production_final.pdf
[5] https://services.google.com/fh/files/misc/google_forrester_bot_management_tlp_post_production_final.pdf
[6] https://www.dla.mil/About-DLA/News/News-Article-View/Article/3106718/fraud-trends-to-look-for/
[7] https://www.helpnetsecurity.com/2020/05/22/large-scale-ato-attacks/

At a time when inflation and other macroeconomic headwinds are squeezing already tight ecommerce margins, these losses can be the difference between thriving and barely (or not) surviving. In this full context, it becomes clear:

Business leaders can no longer afford to ignore ATO and bot fraud as core business problems.

Why conventional CAPTCHA isn't cutting it

The most well-known and visible anti-fraud technologies are the classic CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) challenge-response tools. Though these image challenges have evolved and remain a widely used component of anti-fraud programs, conventional CAPTCHA challenges are becoming less popular for several reasons:



The bots are getting better	Sometimes, it's not a bot	Customers are growing more frustrated
As the AI used by fraudsters gets smarter, the fraud bots can increasingly overcome many CAPTCHA challenges.	The $8 trillion business of cybercrime has birthed new services like "CAPTCHA farms." Fraudsters can literally outsource the task of completing anti-bot/anti-fraud CAPTCHA challenges to offshore firms that employ hundreds or thousands of real, live humans, completing those challenges to open the gates for fraudsters.	As CAPTCHA challenges get more sophisticated in order to counteract smarter bots, they're reaching a point where they're too challenging for legitimate customers. These overly difficult challenges lead to abandoned transactions and lost revenue.

The ATO balancing act: Customer trust vs. customer experience

Consumers' growing frustration with conventional CAPTCHA challenges speaks to the most fundamental maxim of the cybersecurity world: **Don't let the cure become worse than the disease.** Organizations need to consider fraud management and customer experience simultaneously – not individually, as they are often treated today. In practice with ATO prevention, this involves two main considerations:

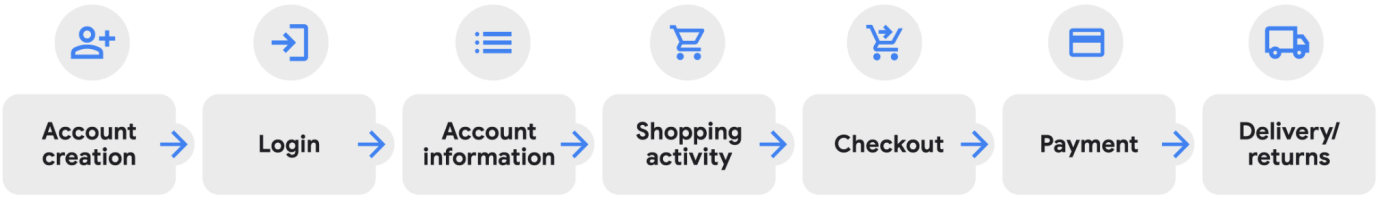
False positives	Excessive customer friction
Following a spate of ATO incidents, or in response to a focused effort to enhance ATO defenses, companies often overcorrect, turning to overly rigid fraud detection tools that can't recognize the nuance of customer behavior or tuning those tools to be overeager in blocking activity. The experience of having legitimate activity flagged or blocked is frustrating. It can cause embarrassment. It can delay or disrupt important purchases or activities. Worst of all, it does little to inspire customer confidence in the business's overall fraud detection capabilities.	Businesses must also be careful and intentional about when and how to add additional steps to authentication workflows for their customers. For example, defaulting to two-factor or multi-factor authentication (2FA/MFA), or too frequently requesting additional authentication factors or validation steps from the customer, often leads to higher levels of cart or transaction abandonment, and can ultimately slow overall customer activity and transaction volume.
33% of consumers say they'd **STOP DOING BUSINESS** with a company that incorrectly flagged legitimate activity as fraudulent[8]	**A QUARTER** of consumers have **ABANDONED PURCHASES** because the checkout process was too long or complicated[9] **80%** of consumers say they likely **WON'T PROCEED WITH A PURCHASE** if asked for additional personal information or documents to validate identity.

The bottom line is that businesses need to understand what their customers will tolerate. They must carefully strike a balance between mitigating the potential revenue losses of under-active fraud prevention and mitigating the potential revenue losses from overbearing fraud prevention.

[8] https://www.digitalcommerce360.com/2020/07/16/33-of-us-consumers-drop-retailers-after-a-false-decline-heres-how-to-prevent-those-losses/
[9] https://baymard.com/lists/cart-abandonment-rate

Validating the human factor across the entire buying journey

To combat bot-driven ATO, companies must embrace new, frictionless ways to validate the human factor. Enterprise security and risk leaders need to rethink their approaches to fraud prevention by moving beyond traditional CAPTCHA tools and expanding their fraud prevention efforts to the entire customer journey. Moreover, security and risk leaders must broaden their focus from the traditional and most obvious points of attack (login and checkout) to look for signals of fraudulent activity across the customer account and shopping journey:



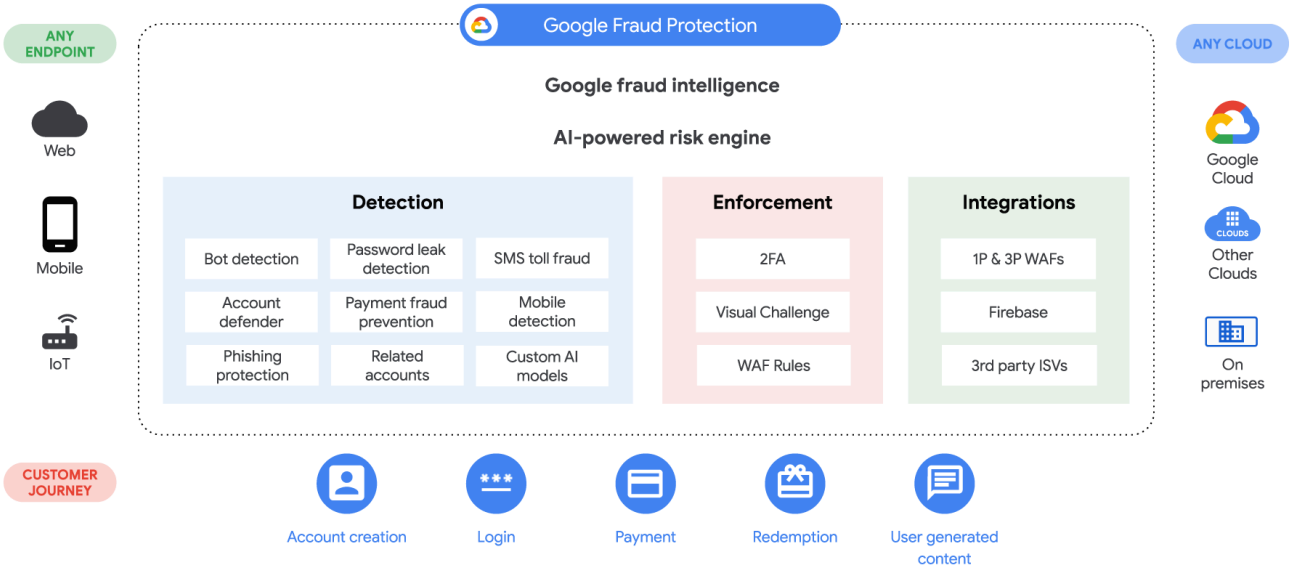
Beyond magic bullets: An integrated, multi-layered ATO defense

To move forward securely, modern enterprises need a comprehensive, multi-layered approach to ATO mitigation that can address fraud. Furthermore, this multi-layered approach must be fully integrated – not a patchwork of point solutions and isolated risk signals. By achieving this level of integration, companies can effectively utilize modern AI and ML technologies to thwart fraudulent activities with a full spectrum of fraud and bot detection capabilities, including:

Password leak detection	Automation detection	Profile matching	Behavior-based detection
Tools to immediately alert if usernames and/or passwords have been compromised.	Tools that identify signals of automated (high-speed and/or high-volume) bot activity within an account.	Profile matching to reduce friction for legitimate users while increasing friction for attackers (bots or humans)	Site- and user-specific behavior modeling to identify anomalous/suspicious behaviors or changes in activity patterns.

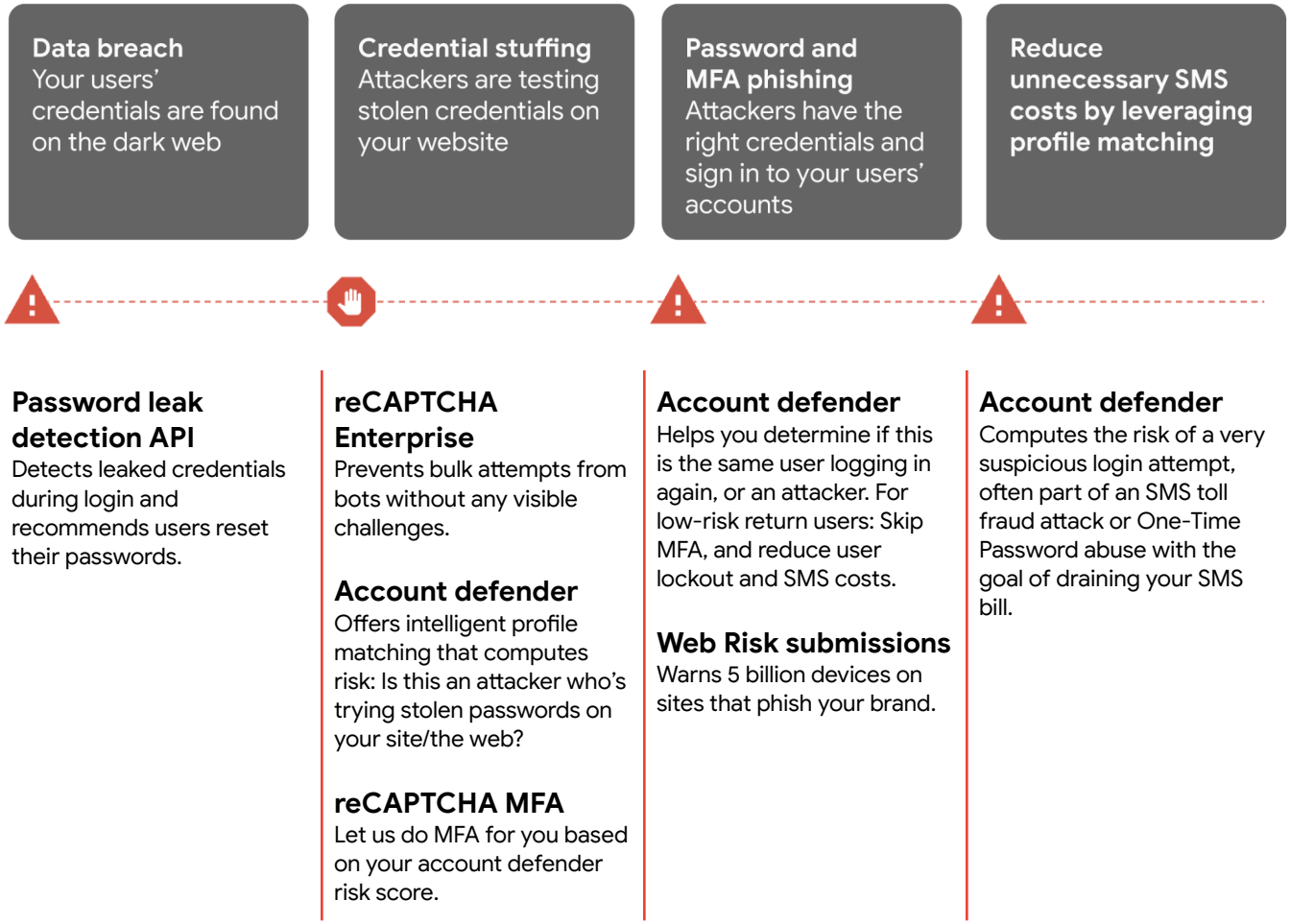
A future-ready, fully integrated solution: Google Fraud Protection

Google reCAPTCHA has long been among the most recognized and trusted anti-fraud challenge technologies. As the threat landscape has grown in size and complexity, Google has continued to evolve our best-in-class security tools to enable the multi-layered approach our partners need – with the centralized control, visibility, and simplicity of one holistic solution. That comprehensive offering, **Google Fraud Protection**, combines reCAPTCHA and Web Risk solutions into a single, future-ready fraud prevention solution – designed to to stop sophisticated phishing, bot, bulk account registration, account takeover, and payment fraud attacks. Perhaps most importantly, Google Fraud Protection provides an invisible layer of protection and frictionless experience for users, striking the critical balance between protecting customer trust and avoiding customer frustration.



How it works: Addressing every stage of the ATO supply chain

The following graphic illustrates how the comprehensive Google Fraud Protection solution offers targeted, multi-layered security at each stage of the ATO supply chain. Risk indicators from each component are integrated into a centralized view, which uses AI-driven risk scoring to generate more precise and relevant alerts.



1) Every user/customer login receives a risk score based on global and site-specific models.
2) Proximate user/customer activity is risk-scored using profile matching models.
3) Discrete risk scores are correlated into broader risk alerting models – connecting small dots into notable risks.

4) When a discrete or aggregate risk score drops into suspicious levels, the solution can automatically trigger a request for 2FA/MFA.

5) If a customer attempts a login with a known compromised credential, the solution integrates with web application firewalls to prompt a password reset with 2FA/MFA request to ensure the reset is executed by a legitimate user.

Modeling legitimate user behaviors, too

One key factor in improving fraud detection while mitigating the risk of false positives: Leading solutions like Google Fraud Protection not only build models to recognize and surface signals of suspicious or fraudulent activity; they also build models of legitimate user behaviors. The Account Defender tool goes to the user level to provide balanced insights. For example, an activity pattern may be a 40% match with the fraud model but represent an 80% match a user-specific behavior model—strongly suggesting that this specific activity is more likely that of the legitimate user.

Ready to modernize your approach to fraud prevention?

Learn more about how Google Fraud Protection equips your business with the full, integrated suite of AI-powered and purpose-built tools to combat today's sophisticated bot fraud, thwart rising ATO attacks, and stay ahead of evolving fraud techniques and tactics. See how you can strike the powerful balance of simultaneously protecting customer trust and customer experience—to not just mitigate downside, but drive measurable upside through increased sales, revenue, and lasting customer loyalty.

Learn more about reCAPTCHA today

For more insights into mitigating account takeover and bot-driven fraud, we invite you to explore the complete report by clicking **here**.