Google Cloud

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

Index

Overview

Broadening defense against accelerating risk – without compromising customer experience

The expansion and acceleration of our digital lives has always fueled the big business of cybercrime. However, in today's landscape, the relationship between legitimate market innovation and illicit or dark web opportunity has grown even more insidiously symbiotic: The same innovations and technologies that power our digital transactions also provide the tools for malicious actors to advance the tactics that allow them to compromise those transactions.

Automation, artificial intelligence (AI) and machine learning (ML) are opening new frontiers for cybercriminals. Bots have become essential tools in account takeover (ATO) attacks, allowing hackers to rapidly test large volumes of stolen credentials to commit payment fraud at large scale. This constitutes just one facet of the larger ATO problem. 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]

The repercussions of these attacks extend beyond financial losses – they erode customer trust and harm a company's reputation. With economic volatility putting new and evolving pressures on both the top and bottom line, business leaders are increasingly recognizing ATO and bot fraud as a core business problem.

One fundamental cause of ATO remains incredibly simple: password reuse. But the solution is far from obvious. Businesses can't afford to add excessive friction to customer transactions, even in the name of security. When fraud prevention measures are overly zealous, they generate false alarms that push customers away and prompt them to give up on transactions altogether. Striking the right balance is crucial: managing the loss of revenue from fraud while also avoiding the loss of revenue from excessive and overbearing fraud prevention measures.

To combat bots and ATOs, companies must embrace new, frictionless ways to validate the human factor. Classic CAPTCHA challenge-response tests have traditionally provided this assurance, but these tests are vulnerable to more sophisticated human and human-like attackers. To adapt, enterprise security and risk leaders need to rethink their approach to fraud prevention by moving beyond traditional CAPTCHA tools and expanding their fraud prevention efforts to the entire customer journey.

---

[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/

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.

Surging cybercrime: The world's fourth-largest economy

The last decade witnessed the greatest transfer of economic wealth in history. The winners weren't celebrated tech innovators, but rather cybercriminals. Since 2015, when annual global profits from cybercrime reached an alarming $3 trillion,[4] this nefarious industry has been growing at a rate of 15% year over year. It is expected to have reached $8 trillion in 2023[5] and is on track to hit $10.5 trillion annually by 2025.[6]

This seismic redistribution of wealth has primarily impacted business-to-consumer organizations and their customers. A global study reveals that, on average, companies lose 5% of their annual gross revenue to various forms of fraud.[7] Ecommerce fraud alone will have cost businesses more than $48 billion globally in 2023.[8]

Bot-driven fraud accelerates account takeover (ATO) attacks

Account takeover (ATO) and bot-driven fraud represent two of the most significant and fastest-growing threats. As AI and automation rapidly advance, the two grow increasingly interrelated.

ATO, which involves the unauthorized access and misuse of account information to carry out harmful actions or access sensitive data, accounts for roughly a quarter of all identity-related fraud.[9] On an individual level, this means that 22% of U.S. adults – or more than 24 million households – have

[4] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[5] https://www.forbes.com/sites/chuckbrooks/2023/03/05/cybersecurity-trends--statistics-for-2023-more-treachery-and-risk-ahead-as-attack-surface-and-hacker-capabilities-grow/?sh=4d95a6cf19db
[6] https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
[7] https://www.dla.mil/About-DLA/News/News-Article-View/Article/3106718/fraud-trends-to-look-for/#:~:text=The%202022%20report%20estimates%20that,created%20new%20opportunities%20for%20fraudsters
[8] https://www.juniperresearch.com/press/ecommerce-losses-online-payment-fraud-48bn
[9] https://risk.lexisnexis.com/about-us/press-room/press-release/20220106-annual-true-cost-of-fraud-study

been victimized by ATO attacks.[10] A report from 2021 estimated that ATO fraud resulted in a loss of $11.4 billion for US consumers, a number that has likely risen in subsequent years.[11]

The rise of bot-driven fraud has catalyzed and expanded the impacts of ATO. 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.[12] Cybercriminals increasingly leverage bots to perpetrate sophisticated credential theft schemes, as well as to leverage those stolen credentials to perform various fraudulent activities, such as fake account creation, fraudulent transactions, and spreading misinformation.

Breaking down ATOs

HOW IT HAPPENS

Attack vectors	Attack techniques
• Weak and/or reused passwords • Compromised credentials from data breaches • Social engineering (such as phishing, spearphishing)	• Credential stuffing • Brute-force attacks • Exploitation of password reuse

WHAT IT LEADS TO

- Direct financial gain (that is, making purchases, reselling goods)
- Data exfiltration
- Espionage

[10] https://seon.io/resources/statistics-account-takeover-fraud/
[11] https://javelinstrategy.com/press-release/identity-fraud-losses-total-52-billion-2021-impacting-42-million-us-adults
[12] https://services.google.com/fh/files/misc/google_forrester_bot_management_tlp_post_production_final.pdf

Four factors behind the ATO surge

The ATO attack pattern has skyrocketed to the top of priority lists for enterprise risk and security teams. Research from Javelin Strategy shows ATOs growing in frequency by 90% year over year, with a corresponding 90% increase in annual ATO losses.[13] Indeed, half (48%) of enterprises have already experienced measurable revenue losses due to ATOs.[14]

What's behind the ATO surge? These four key drivers: The human factor, increasing data breaches, bigger paydays, and AI and automation.

1) The human factor: Identity sprawl and password reuse

Stolen credentials account for more than 80% of breaches on web applications for reasons that are incredibly simple: password reuse and poor password hygiene.[15] The majority of people (66%) reuse passwords and other login credentials across multiple (and often all) online accounts.[16] It's less than surprising, then, that 60% of ATO victims used their compromised password across multiple accounts. "Identity sprawl" is amplifying this problem. As accounts proliferate, consumers struggle to keep track of their sprawling digital identities and are less likely to notice when an account is taken over. On the other side of the equation, when fraudsters compromise one set of credentials, they're effectively getting the keys to several (or all) of that consumer's digital accounts.

2) Increasing data breaches: Ready access to stolen credentials

The negative impacts of ATO are not limited to the organization that was breached. Hackers often leverage credential theft by selling the stolen information on the dark web to be reused across multiple sites. In fact, research shows the market for access broker services – the illicit organizations that facilitate the buying and selling of stolen access credentials – is growing rapidly. One clear sign: A 2023 report showed a 112% year-over-year increase in advertisements for access broker services.

[13] https://javelinstrategy.com/2022-Identity-fraud-scams-report
[14] https://services.google.com/fh/files/misc/google_forrester_bot_management_tlp_post_production_final.pdf
[15] https://www.verizon.com/business/resources/reports/dbir/
[16] https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/PasswordCheckup-HarrisPoll-InfographicFINAL.pdf

3) Bigger paydays: Digital accounts represent a bigger pot of gold

The average consumer stores and manages an extraordinary amount of personal value online: credit card, bank accounts and other financial information; personal identification data, including social security numbers; property ownership and tax information; health records; and more. As brands look to build loyalty, they often encourage consumers to grow that value in the form of perks – rewards points, cash-back bonuses, free shipping, and more – that further attract the attention of hackers. Once a threat actor is in control of an account, they can use loyalty points to make purchases, perpetrate return fraud schemes, and use compromised passwords to take over other accounts. This careful, multi-pronged approach can be difficult to catch and lead to prolonged financial damage.

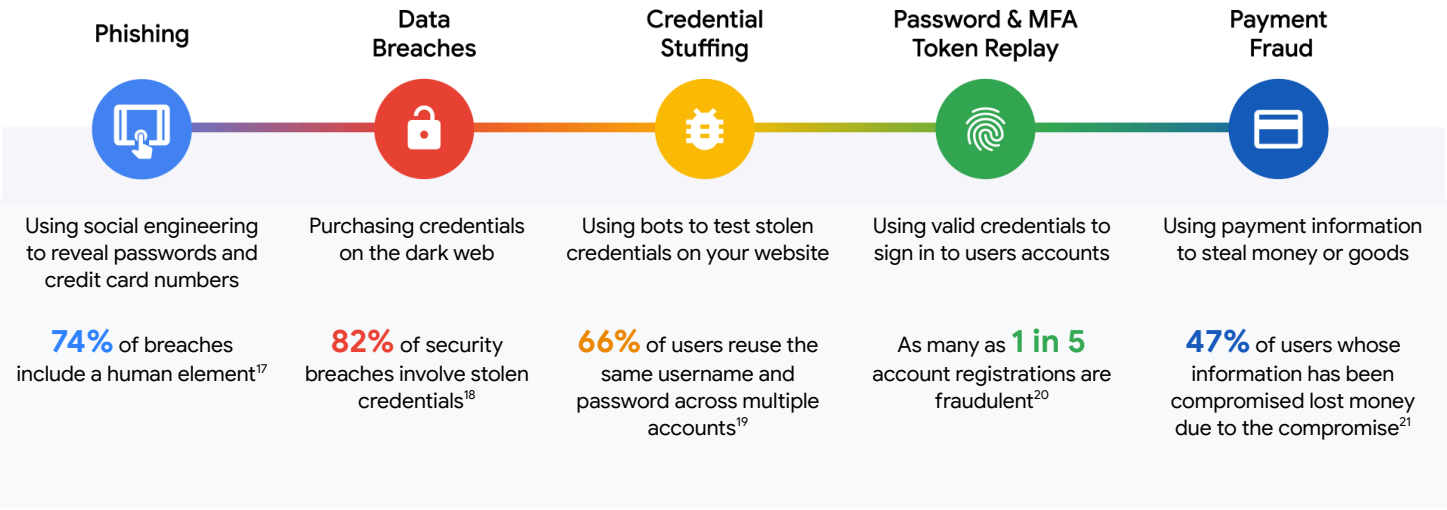
4) AI and automation: Scaling up is cheap and easy

AI-powered automation makes it cheaper and easier than ever to scale ATO attacks and bot-driven fraud. For example, the modern APIs that streamline the creation of mobile apps can also be used by fraudsters to build and run bot farms. Simple automated scripts can perform ATO tasks at unprecedented scale. Tools like SNIPR and Sentry MBA, for example, can facilitate automated credential stuffing attacks. Generative AI tools can create better phishing and spear phishing messages at an exponentially accelerated pace. Fraudsters can even use automation to get around multi-factor authentication with tactics like "OTP interception as a service." As automated tools attempt to use stolen credentials to log in, they simultaneously contact the legitimate account holder with a personalized message designed to extract their one-time login code.

Critically, the speed and scale of these AI- and automation-driven attacks enable the fraud to advance ahead of manual detection – and move too quickly even for many conventional fraud detection technologies.

Bots and beyond: Understanding the ATO supply chain

The core of ATO lies within the targeted account and its inherent value. However, unlike many forms of cybercrime, ATO is not a single, isolated event. Instead, attackers follow a methodical process: They steal credentials, verify their authenticity, take over the account, engage in fraudulent activity, and then do it all over again. This cycle can involve repeated fraudulent actions on the same account before the business or individual realizes what's happening. Additionally, the attacker may use other stolen credentials to carry out similar ATOs and fraudulent activities across the victim's other online accounts, either subsequently or at the same time.



The multi-step, persistent approach that characterizes the ATO lifecycle is what makes it financially rewarding for attackers. **However, this complexity also offers multiple opportunities for detecting and stopping the fraud. ATO is not a quick, one-off event – and neither is the process of detecting it**. The sooner in its lifecycle an ATO attack is discovered, the less harm it will cause, both in terms of financial loss and reputational damage for the business, as well as for the individual account holder.

[17] Verizon DBIR
[18] Data Breach Investigations Report 2008 2022
[19] Google Harris Poll
[20] Helpnet Security
[21] Google Harris Poll

Cascading business impacts of ATO and bot fraud

For years, consumer-focused businesses have considered "shrinkage" and other types of fraud as more-or-less inevitable costs of operation. This mindset has extended to digital fraud and cyberattacks, particularly as digital transformation has accelerated in the post-pandemic world. Companies have adopted a philosophy of "risk tolerance" or "acceptable risk," choosing to prioritize speed, agility, and customer experience, even if it means accepting a certain level of fraudulent activity.

Still, it's critical to understand and quantify the significant business costs of ATOs, bot attacks, and other forms of digital fraud. 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. Most immediately, however, **ATO and bot fraud are both major revenue drains that drag down profitability**. Though some estimates quantify typical fraud-related losses at 5% of annual gross revenues, the reality is that, for roughly half of companies, that figure may be much higher.[22]

A substantial part of this additional 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. [23] These snowballing reputational effects are long-lasting, painful, and extremely difficult to manage.

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 that better digital fraud prevention is simply better business.

[22] https://www.dla.mil/About-DLA/News/News-Article-View/Article/3106718/fraud-trends-to-look-for/
[23] https://www.helpnetsecurity.com/2020/05/22/large-scale-ato-attacks/

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. These image challenges have evolved over the 26 years since their first commercial application in 1997, but the basic idea remains the same: validate the human factor; determine if there is a real, live human attempting to log in or make a purchase; and stump the bots.

CAPTCHA technologies remain a widely used and effective component of an anti-fraud program. But conventional image challenges are becoming less popular for several reasons:

- **The bots are getting better:** As the AI used by fraudsters gets smarter, the fraud bots can increasingly overcome many CAPTCHA challenges.

- **Sometimes, it's not a bot:** 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.

- **Customers growing more frustrated:** As CAPTCHA challenges get more sophisticated 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 one of the classic maxims 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' 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[24]	**A QUARTER** of consumers have **ABANDONED PURCHASES** because the checkout process was too long or complicated[25] **80%** of consumers say they likely **WON'T PROCEED WITH A PURCHASE** if asked for additional personal information or documents to validate identity.

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

Tolerance varies by industry, but balance is key

Of course, customer patience varies by industry. Higher-friction authentication workflows and challenge-based approaches are more tolerated by customers in insurance, banking, and healthcare – where customers' perception of risk to their sensitive information is greater. But they're much less tolerant in sectors like ecommerce, travel, and entertainment – where basic consumer desire for immediate gratification reduces their patience.

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.

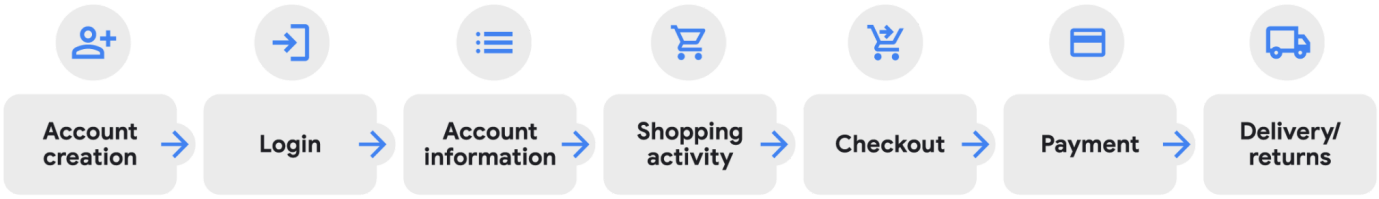
Beyond magic bullets: Building a multi-layered ATO defense

Flaws of conventional CAPTCHA aside, the broader reality is that the complexity and growing sophistication of cyber attacks – and ATO attacks, in particular – makes it virtually impossible for any one single security tool to be 100% effective. Top security experts advocate for a layered approach that goes beyond simple image challenges to provide additional 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 behavior or changes in activity patterns.

Protecting the entire buying 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:



Patching point solutions < Integrating high-fidelity risk signals

More and more enterprise security teams are embracing this multi-layered approach to ATO and bot-fraud prevention, which is fueling an expanding market for various point solutions that occupy the layers of defense.

However, this layered approach poses its own set of challenges to security and risk teams. From an administrative standpoint, the task of managing multiple tools and vendor contracts can become complex and time-consuming. Operationally, this problem manifests as alert fatigue. Overwhelmed by the plethora of alerts coming from various sources, security teams may fail to discern which warnings are critical and need immediate attention.

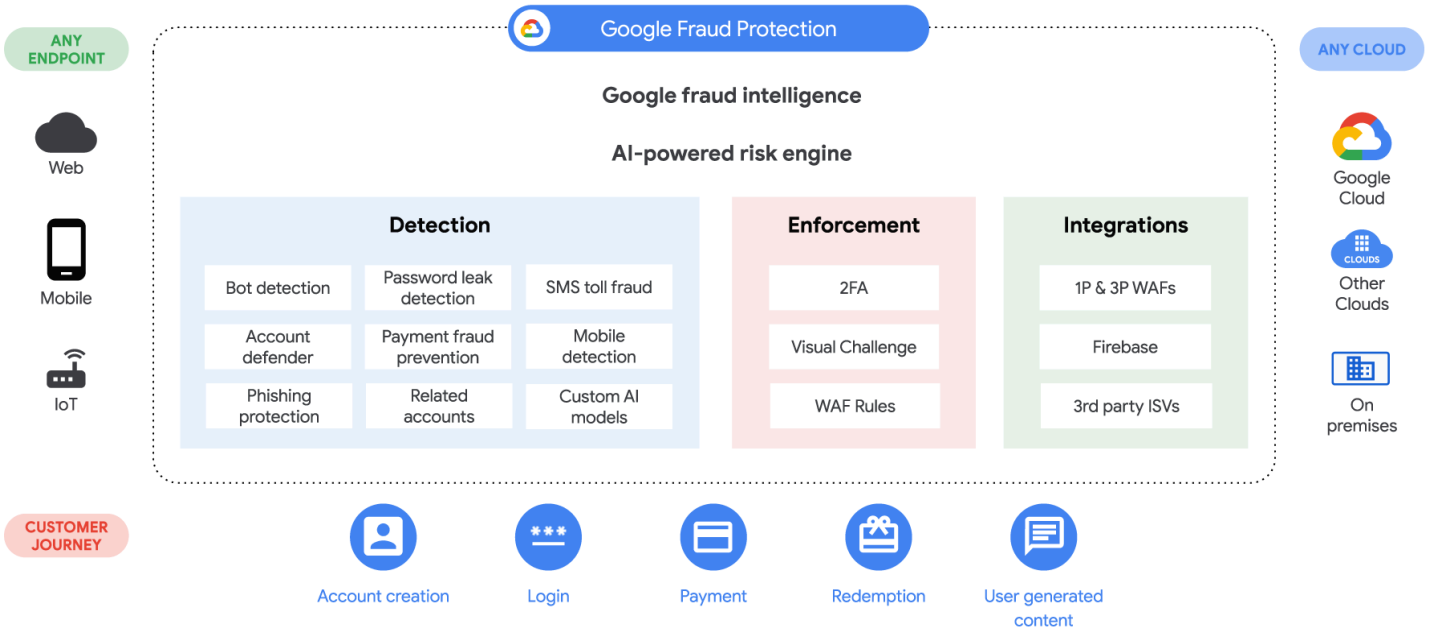
More troublingly, the point solution may overlook key connections between risk signals. As bots grow more advanced, fraudsters get more sophisticated and attack patterns become more nuanced – better at hiding their tracks and moving more slowly, patiently, insidiously. It's incredibly difficult to manually patch together these subtle risk signals and connect the small dots that add up to a big risk – and it's nearly impossible to do that at the speed and scale of the typical enterprise risk landscape.

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

Google has been at the forefront in helping to combat cyber attacks and other forms of digital fraud for more than two decades. Our reCAPTCHA offering 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 market-leading security offering to protect our partners and their customers. One front of that innovation involves advancing our discrete security tools: For example, creating a next-generation anti-bot, anti-ATO technology called Google reCAPTCHA, combining features like account defense, password leak detection, and profile matching with AI-powered pattern recognition to detect bots without requiring tedious and fallible user challenges.

The other front focuses on natively connecting our best-in-class 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 protection solution – purpose-built to protect against sophisticated phishing, bot, bulk account registration, account takeover, and payment fraud attacks. Leveraging Google fraud intelligence and AI-powered detection at each stage of the attack lifecycle, Google Fraud Protection features bot-stumping and bot-detecting technology that's evolved from visual challenges to an invisible, frictionless experience for users while delivering reliable effectiveness in stopping bots and account takeovers. This new breed of enterprise anti-fraud solution is purpose-built to strike the balance between protecting customer trust and avoiding customer frustration.

A modern fraud protection platform to protect against ATOs across the entire customer journey



Putting AI back on the side of the "good guys"

Fraudsters are using advanced AI to perpetrate more sophisticated attacks. But Google Fraud Protection brings the modern sophistication of AI and ML back onto the side of the "good guys." Google Fraud Protection harnesses the immense power of Google's global footprint to recognize broad trends and patterns — and then add site- or application-specific depth to that knowledge by bringing together signals from across the customer journey to develop smarter, more effective, and more reliable risk scoring models:

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.

Global insights

- Signals from reCAPTCHA tools installed on more than 7 million websites
- Insights from 150 million Google Payment transactions worldwide
- Cybersecurity trends and patterns from around the globe
- Google's real-time updated database of over 5B compromised credentials

Site-specific models

- Training AI models to recognize normal vs. abnormal behavior patterns for each specific site, application, or business
- AI-powered, user-specific profile matching based on historical user/customer behavior patterns

Intelligent risk scoring

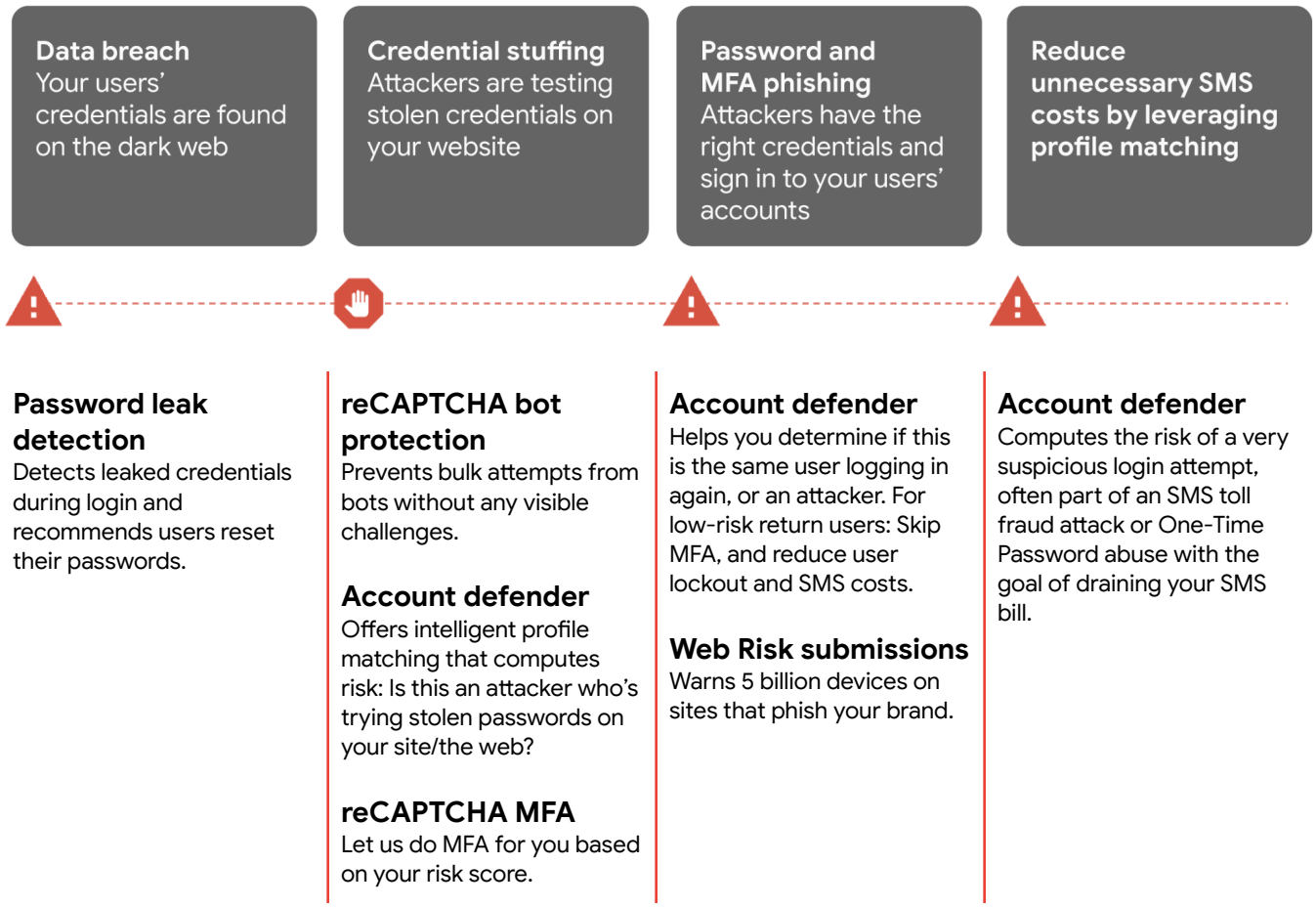
- Risk scoring at different points in the customer journey (account creation, login, checkout, and so on)
- Objective 0–1 scoring: 1 is definitely human; 0 is definitely a bot
- Risk scoring for password leaks

Automated action

- Triggering 2FA/MFA requests when login/checkout risk scoring trips threshold
- Prompting password reset for known compromised credentials
- Flagging and/or locking accounts when risk scoring predicts high likelihood of fraud

Google Fraud Protection in action: 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.

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