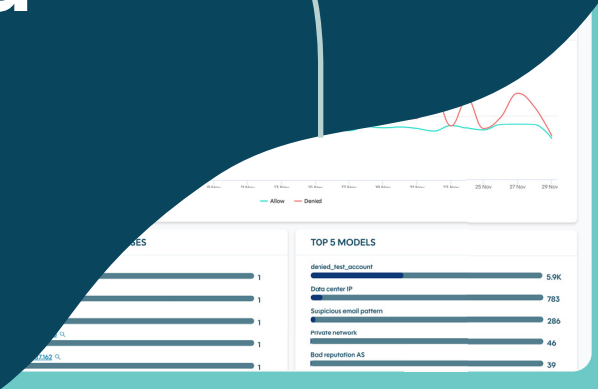
DataDome | ACCOUNT PROTECT
PRODUCT BRIEF

Stop account fraud before it happens



End account fraud once and for all

Account fraud—the practice of account takeovers and fake account creation—is a damaging yet persistent problem for many organizations.

> '"ATOs remain a persistent issue wherever there is a digital login with something of value behind it'... 'organizations and users continue to fall victim to ATO attacks that lead to a range of negative outcomes including financial losses, brand damage, data loss, ransomware attacks, and regulatory fines.'"
>
> **- Gartner®**

The problem

Fraudsters have intensified their attacks by adding tactics led by real users, targeting login and registration endpoints. By exploiting weaknesses in authentication protocols or by hijacking existing user accounts, they can bypass safeguards designed to prevent fraudulent account creation.

The negative consequences of account fraud can be significant, including:

- ✖ **Personal data (PII) breaches and customer loss**, including harvesting PII.
- ✖ **Financial losses** from fraudulent purchases, **chargebacks**, and **stolen value/rewards**.
- ✖ **Brand damage** from poor user experiences and **loss of credibility**.
- ✖ **Compliance risk, notification costs, and regulatory fines** (e.g., GDPR, FTC CFR, SEC Rule 10).
- ✖ **Wasted time and resources** for fraud disputes, recovery, and customer service.

The solution

Account Protect offers unmatched protection against account fraud from the first attempt. Unlike other account takeover (ATO) solutions that rely on limited server-side signals, Account Protect collects user-centric and business data signals to create a digital footprint of user behavior. Using advanced detection techniques, it analyzes new signals collected directly from your application, including user-specific identifiers like email addresses and geographical locations, in real time and over a meaningful timeframe, to draw accurate insights in milliseconds.

It operates on auto-pilot, integrating with authentication processes like automatic password resets and multi-factor authentication, ensuring accounts are secure from creation to ongoing use.

- ✔ **Evaluate the risk** of account takeovers and fake account creations with greater precision.
- ✔ **Mitigate financial loss and gain back valuable** time from cross-functional investigations.
- ✔ **Gain explainability and transparency** into our recommended actions and the pattern of attacks.
- ✔ **Ensure full compliance** with privacy regulations that exceed the standards set by GDPR and CCPA.

Gartner, How to Mitigate Account Takeover Risks, Akif Khan, Ant Allan, Dan Ayoub, 15 May 2023. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

FORRESTER® WAVE LEADER 2024 Bot Management Software

Advanced detection for enhanced account security

Elevate your security measures through comprehensive analysis

Detecting account fraud is complex and requires a thorough analysis of user data to build a clear profile of intent. Without a robust solution in place, customer accounts may encounter security vulnerabilities like:

Theft of store credit or reward points/miles

Attackers gain access to someone else's account or exploit vulnerabilities in the system to fraudulently obtain or redeem credits, points, or miles for their benefit.

Illicit purchases with the existing card on file

Attackers gain access to a user's account or payment information without authorization and use it to make purchases without the cardholder's knowledge or consent.

Theft of personal data, often to resell or use in othe attacks

Attackers use stolen data for various malicious purposes, including identity theft, financial fraud, phishing scams, and other cybercrimes.

Exploitation of new member offers

Attackers misuse or abuse promotional incentives and benefits provided by businesses to attract and incentivize new customers or members.

Card testing

Attackers attempt to validate stolen credit card information by making small, unauthorized transactions or "test" purchases in unauthorized accounts.

Spamming & influence fraud

Attackers misuse compromised accounts to disseminate unsolicited or malicious messages, links, or content.

Proven results

DataDome's Account Protect successfully tackled a leading customer brand's issue with fraudulent online bookings, **revealing 75% of sign-ups as fake.** Implementing DataDome significantly decreased no-shows and boosted genuine customer interactions, **with an impressive false positive rate of 0.00091%.**

Account Protect offers proactive defense against automated threats, allowing businesses to focus on growth by securing their digital environment efficiently.