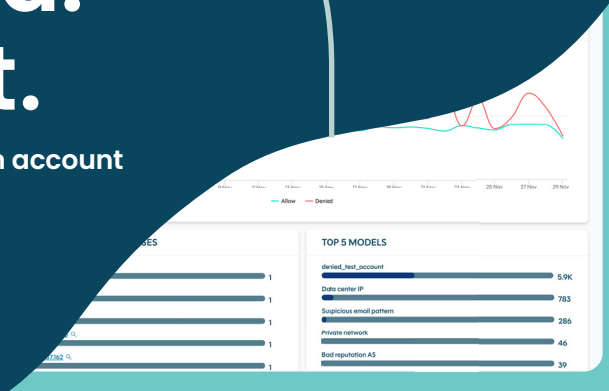
DataDome | ACCOUNT PROTECT
PRODUCT BRIEF

Stop Account Fraud. Preserve user trust.

Verify authenticity and intent in real time to secure logins from account takeovers and stop fake/malicious AI-generated accounts.



Real-time defense against ATOs and fake accounts

> "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®**

Digital accounts power nearly every online interaction, making them a prime target for fraud.

The problem

Attackers today move quickly and blend AI-driven automation with human-in-the-loop tactics to evade static defenses, often going undetected until damage is done. They hijack accounts by exploiting stolen or guessed credentials through techniques like phishing, credential stuffing, and brute-force attacks, then lock out legitimate users by changing passwords or recovery details. At the same time, fraudsters create fake accounts at scale with synthetic identities, disposable emails, and phone farms, driving scams, promo abuse, and payment fraud that drain revenue and damage customer trust.

The solution

Account Protect stops both account takeovers and fake account creation by verifying not just who users are, but also what their intent is, continuously, even after login. This smart, AI-driven solution safeguards brand reputation by detecting and blocking fraud in real time, stopping abuse before it spreads, and helping businesses reduce identity theft, chargebacks, and manual review costs up front, not after the damage is done.

Powered by advanced AI models, including **genetic algorithms** and **dynamic baseline learning**, Account Protect continuously adapts to new attack tactics and delivers precise protection against both automated and hybrid threats.

With DataDome, customers can also leverage the collective intelligence of our global network to reinforce their fraud monitoring, ensuring stronger protection against even the most advanced attacks.

Where Account Protect Makes the Difference

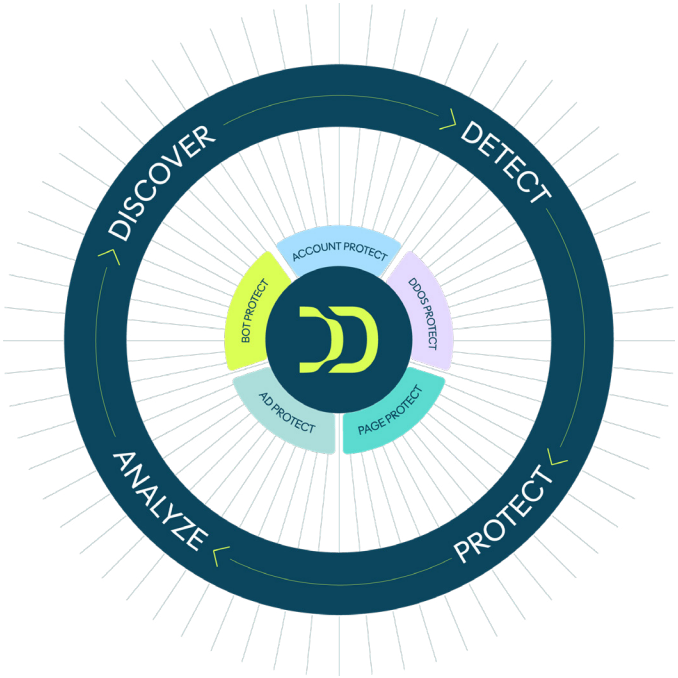
- **Block Fraud Before It Spreads:** Detect and stop account takeovers and fake accounts in real time—before they can escalate into identity theft, scams, or revenue loss.
- **Give Fraud Teams Instant Clarity:** Eliminate blind spots with a unified view of every account action. Automate your workflow so repetitive investigations and approvals happen seamlessly. Decisions are faster, smarter, and fully in your control.
- **Cut the True Cost of Fraud:** Prevent downstream damage like chargebacks, loyalty abuse, and reputational harm by breaking the fraud chain early, reducing manual reviews, and consolidating point solutions.
- **Tailored Defenses at Scale:** AI models adjust to each customer's unique traffic patterns, delivering precise protection against both automated and human-driven threats without added friction for legitimate users.

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

How it works.

Account Protect combines four powerful, real-time capabilities to detect and prevent account takeovers and fake account creation:



Collect: Continuous Behavior Monitoring

- Tracks user activity across logins and sessions
- Gathers technical signals (IP, browser, network) and business signals (account details, transaction context)

Detect: Smart Risk Scoring

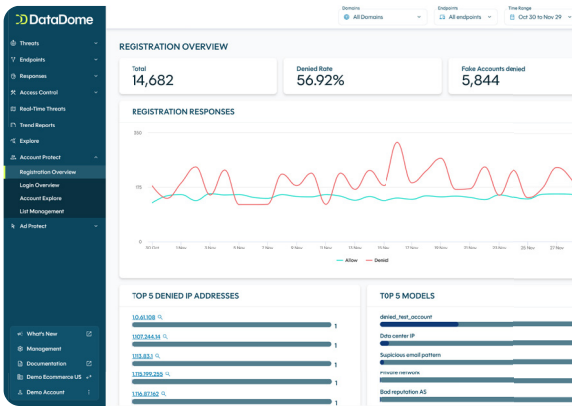
- Analyzes collected signals to accurately assess user intent and surface actionable insights
- Flags risky behavior like disposable emails, reused phone numbers, or devices tied to multiple accounts
- Uses AI-driven models to detect anomalies across IPs, browsers, and logins—even when signals appear valid
- Continuously adapts to evolving fraud tactics while keeping legitimate users moving seamlessly

Act: Tailored Business Logic Responses

- Integrates directly into existing workflows.
- Provides real-time recommendations to allow, deny, challenge, or flag activity.
- Supports flexible defense strategies
- Protects without unnecessary friction for genuine users.

Learn: Self-Learning System

- Continuously improves via feedback loops that incorporate confirmed fraud outcomes and false positives.
- Establishes dynamic thresholds on key traffic signals, automatically recalibrating per customer and endpoint to detect anomalies before fraud occurs.
- Flags anomalies like mismatched locations, unusual timing, or repeated use of disposable emails and disposable phone numbers. devices.
- Prevents downstream damage by intercepting fraud at the earliest stage.



Uncovering Attacks in Progress

Account Protect monitors for subtle, high-risk signals that emerge after login, catching fraud in progress before it spreads.

Credential or contact changes

- Attackers may reset passwords or update recovery details to lock out legitimate users.

Payment and profile edits

- New cards, shipping region changes, or loyalty profile updates may indicate fraud preparation or exploitation.

Login method switches

- Changing the way an existing account is accessed (e.g., from email to SSO) can signal token theft or takeover attempts.

Behavioral inconsistencies

- Trusted devices or accounts showing unfamiliar usage patterns may indicate compromise operating under the radar.

Real-World Results

Vinted: Protecting Millions in Revenue

Vinted faced over 100,000 fake accounts per week, driving scams, fake listings, and phishing that eroded user trust.

- **95% reduction** in fake account creation within 3 months
- Marked drop in unauthorized listings and fraud across web and mobile
- **0.7% false positive rate**, ensuring minimal disruption for legitimate users
- Significant time savings for fraud teams and stronger overall protection

Luxury Retailer: Safeguarding High-Value Bookings

A global luxury retailer was hit by a surge in fake bookings—over 80% of daily appointment slots were blocked by bots, preventing real customers from booking.

- **90% reduction** in fake bookings
- Detected 70% of hybrid human + bot fraud attempts
- Scaled seamlessly to handle **150K–300K appointment requests per day**

SoundCloud: Fighting Influence Fraud

SoundCloud struggled with fake plays, likes, and spam that damaged brand perception and fueled influence fraud.

- Real-time bot mitigation stopped fake engagement
- Advanced detection of human-driven fraud
- Stronger protection through shared insights—eliminating silos