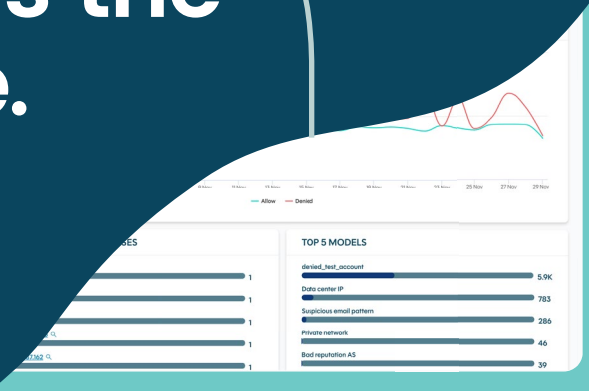
DataDome | ACCOUNT PROTECT
PRODUCT BRIEF

The account layer is the new attack surface.

As credential-based attacks scale and threats grow more sophisticated, stronger authentication isn't enough. Organizations need account-level behavioral intelligence to detect misuse the moment it begins.



> "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®**

Detect account fraud where it starts. Not where it surfaces.

Analyze behavioral intent in real time to detect account takeovers and prevent fake account creation before fraud cascades downstream.

The gap in your security stack

AI has industrialized account takeovers. Attackers are faster, more adaptive, and harder to detect and the technology stacks built to keep attackers out leave one critical question unanswered: after authentication succeeds, is the account being misused?

The reason that question goes unanswered is structural:

- Stolen credentials reveal intent through behavior, not through the login event itself
- Synthetic identities pass registration looking identical to real new users — to every downstream system

By the time fraud surfaces at the transaction layer, the damage is already done.

Catch what authentication misses

Account Protect combines signals from the current event with prior activity and account context to assess risk before the event completes — then continues monitoring to detect misuse as it unfolds.

Perimeter tools, identity platforms, and network infrastructure weren't designed to answer the question that matters most after authentication succeeds: is this account being misused? Account Protect adds that layer, distinguishing trusted activity from adversarial impersonation using account-level behavioral analysis.

Where Account Protect makes a difference

4.2M+

credential-based account takeover attempts detected per month across login, registration, and post-login behavior.

- Server-side and tamper-proof
- Risk decisions in <50ms
- No re-architecture required

Detect account-level threats at the source.

Account Protect's real-time, account-level behavioral analysis catches credential-based attacks and synthetic identity abuse at the point of entry: login and registration. Stop the account attack, and you stop the downstream fraud that follows.

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 2026
Bot And Agent Trust Management Software

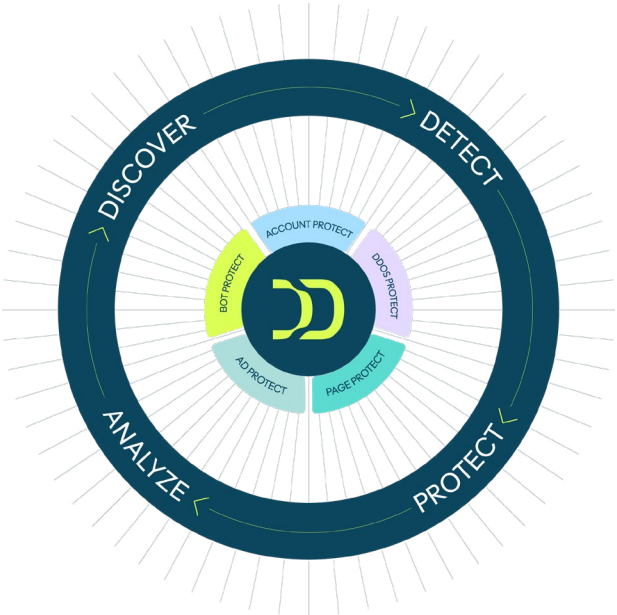
Free your teams from reactive fraud response.

Every downstream fraud loss has an upstream entry point. Account Protect closes it before it cascades. Account Protect works on autopilot after setup. Continuous model learning, clear risk scores, and event-level rationale, not just a flag, mean your team spends less time triaging alerts and more time on what matters.

Eliminate friction for legitimate users.

When a stolen credential looks identical to a returning customer's login, the default is friction for everyone. Account Protect changes that. Account Protect tells your authentication stack when to act and when to stand down. MFA fires only when there's a real behavioral risk signal, keeping the experience frictionless for legitimate users and precise against bad actors.

With Account Protect, on average, only 18% of fake-registration traffic is challenged, meaning real users move through without interruption. Protect revenue at the point where fraud and friction both cost you. Fake accounts don't just cause fraud. They corrupt every downstream metric you make decisions on.



How it works

Account Protect combines four real-time capabilities

Continuous behavior monitoring

Tracks every login, registration, and post-login event against 250+ signals in real time

- 250+ technical and business signals captured per event
- IP, device, browser, network, and more
- Enriched by intelligence from 5 trillion daily events across the DataDome global network

Smart risk scoring

AI-driven models detect anomalies even when individual signals appear legitimate

- Flags high-risk patterns: disposable emails, reused identifiers, devices linked to multiple accounts
- Customer-specific models recalibrate automatically as attack tactics evolve

Tailored business logic responses

Delivers sub-50ms risk recommendations with event-level rationale (not just a score).

- Allow, challenge, review, or deny
- Server-side SDK integrates with no re-architecture, live in days
- GDPR compliant, EU-hosted, SOC II in scope, double-encrypted at rest and application level

A self-learning system

Confirmed fraud outcomes and false positives feedback continuously

- Improves precision without engineering overhead or manual rule maintenance
- Dynamic thresholds recalibrate automatically per customer and endpoint

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

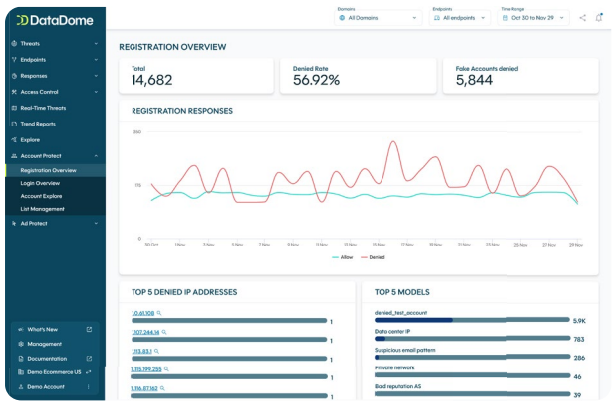
- New cards, shipping region changes, or loyalty profile updates may indicate fraud preparation or exploitation.

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 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
- **0.7% false positive rate**, with minimal disruption for legitimate users
- Significant time savings for fraud teams and stronger overall protection

SoundCloud faced fake account creation that damaged platform integrity and fueled influence fraud.

- **887,000** fake accounts prevented
- Advanced detection of human-driven account fraud
- Stronger protection through shared network intelligence

Coop's retail loyalty program faced credential stuffing attacks, draining loyalty points from real customer accounts.

- **$30,000** in monthly fraud losses prevented
- **250,000+** credential-based attempts blocked per month
- Real-time detection before points could be extracted

OLX, a major European marketplace needed to stop synthetic identity fraud without false positive damage to legitimate users.

- **97%** detection precision on fake account creation
- Account Protect surfaced over **9 million** fake account creation attempts in a single quarter