SOLUTION BRIEF · ECOMMERCE & RETAIL

Securing the Account, Not Just the Transaction

Your bots are blocked. Your payments are protected. Your accounts are the open door.

Darwinium is an agentic security and fraud prevention platform that detects human and agent intent across every digital journey. Most large merchants have solved two problems well: automated traffic at the perimeter, and card fraud at checkout. Fraud has responded by moving to the ground in between. The authenticated account is where credentials are valid, payment methods are already stored, rewards have real resale value — and where neither of those controls is designed to look.

At scale the economics compound. With tens of millions of active customers, a paid membership tier, trade accounts on net terms and cards on file, a compromised account is worth far more than any single fraudulent order. And as agentic shopping moves from pilot to protocol, much of the traffic reaching those accounts is no longer human: **97% of organisations saw AI-assisted fraud attacks rise last year**, yet two-thirds still cannot detect agentic traffic across the full journey.

COVERED
Bot management
Stops automated traffic at the perimeter. Sees one request, with no memory of what came before.

THE GAP
The authenticated account
Valid credentials. Cards already on file. Rewards worth stealing. Neither control is watching.

COVERED
Payment protection
Scores the transaction at checkout — by which point the account is already compromised.

Four Moments That Decide Account Security

JOURNEY MOMENT	THE THREAT TODAY	HOW DARWINIUM RESPONDS
New Account Creation	■ Scripted and agent-driven sign-ups farming welcome offers and referral credit ■ Duplicate accounts from the same devices behind proxies, emulators and cleared cookies ■ Guest checkout used to test stolen cards before an account exists	■ Behaviour read before the form is submitted — how the visitor arrived, browsed and typed ■ Digital Signatures cluster duplicate accounts by similarity, not exact match ■ Sign-up context carried downstream, so a weak registration stays visible at checkout
Login and Account Takeover	■ Credential stuffing slowed deliberately to sit under your bot tool's rate limits ■ Session hijacking and cookie replay arriving after the perimeter check has passed ■ Agentic ATO — AI agents authenticating at machine speed across many accounts	■ Behavioural identification continues after authentication, where credential checks stop ■ Journey Transition Probability scores whether the session's path makes sense for this customer ■ Device Similarity and Trust Score recognise returning shoppers without an OTP
Change of Details	■ Delivery address, email or phone changed ahead of a high-value order to a drop address ■ New payment method added mid-session on an account already holding cards on file ■ Trade account details altered to redirect orders bought on net terms	■ Every change is a risk decision informed by the whole session, not an isolated event ■ Address and payment changes scored against the account's own history ■ Risk-based orchestration — permit, verify, challenge or prevent — in milliseconds
Rewards, Loyalty and VIPs	■ Paid membership tiers and reward balances monetised through takeover or resale ■ Promo stacking, coupon abuse and referral farming that look legitimate one event at a time ■ Returns abuse — wardrobing, bracketing, serial claims — coordinated across accounts	■ Behavioural clustering links reward farming across accounts, devices and sessions ■ Tailored messaging so high-value members meet recognition, not friction ■ Ranked #1 for returns abuse in eCommerce — Liminal research, February 2026

The Darwinium Difference

The layer in between

Darwinium does bot detection and payment fraud too — but most eCommerce teams have those covered. The gap is the session in between, where it adds context before payment.

The journey signal nobody else has

Journey Transition Probability models the shape of a normal journey and scores every step against it. The same signal catches credential stuffing, ATO, promo abuse and agent intent drift.

Built for agents as well as humans

Declared and undeclared agentic traffic separated by behaviour and journey context — so agent-assisted shopping converts instead of being blocked at the door.

Change without an IT project

New touchpoints, journeys and rules are configured by business users in the portal — a new vulnerability covered in hours, not release cycles.

Intent, not just identity

Authentication tells you who. Darwinium tells you why — assessing whether every shopper and agent is acting on genuine, authorised intent.

A new approach to user recognition

Digital Signatures compare behaviour on a scale of similarity rather than a fixed identifier, so recognition survives cookie wiping, proxies and new devices.

Deployed at the perimeter edge

Runs inside the CDN you already use. One deployment covers web, mobile and APIs, with no tags on every page and no application refactoring.

Room to consolidate later

Start as the account security layer alongside your existing stack. Merchants who go on to replace legacy fraud tools see immediate TCO reductions with broader coverage.

Proven in Production

Results from live eCommerce, marketplace and platform deployments.

70%
Of returning-user OTPs saved using Device Similarity and Trust Score

50%
Reduction in fraud by separating trusted from risky behaviour

40%
Greater operational efficiency through edge-based risk decisioning

Bots stopped at source

A global eCommerce platform intercepts credential stuffing, ATO attempts and malicious automation in real time, before they reach customers.

Fake accounts prevented

Fraudulent sign-ups detected across onboarding and guest checkout at the same platform, with behaviour linked across sessions.

Higher conversion

Decisioning welcomes good traffic with less friction, lifting conversion across web, mobile and API.

Promo abuse blocked

Re-recognition across multiple customer tokens prevents fraudulent reward redemptions, replacing the incumbent across registration, login and purchase.

Minutes, not days

A global learning platform surfaces cross-account risky behaviour in minutes — work that previously took skilled analysts hours or days.

#1 for returns abuse

Ranked top vendor for returns abuse in eCommerce strategy by Liminal independent research, February 2026.

> "Darwinium showcased a profound understanding of our requirements. The platform's flexibility is particularly impressive, allowing us to meet the unique needs of our business and our clients."
>
> Senior Manager, Global Fraud — global eCommerce technology company

Ready to see what your accounts look like between login and checkout?

Talk to Darwinium about a tailored account security and revenue impact assessment.

Contact Darwinium at darwinium.com to get started.