IntelliFend

CASE STUDY

Protecting a Marketplace from AI Bots, Scrapers, and Data-Leak Risk

Customer

An Asia-based online marketplace

Industry

Retail

Challenge

At peak campaigns such as Chinese New Year, the marketplace faced surging bot abuse. Phantom searches and cart-adds distorted demand, while scrapers lifted prices and inventory for resale. Scripts locked stock,showing false “sold out” messages, depressing conversions. Logins and loyalty accounts were hit by credential stuffing, while stolen-card tests drove cancellations and chargebacks. Bot storms imitating peak traffic strained servers, slowing pages and harming user experience. These attacks eroded trust, revenue, and compliance confidence.

Result

With IntelliFend, results were immediate. Inventory-locking and scalper bots dropped to negligible levels, removing false “sold out” notices. Credential-stuffing success fell by 60-70% with risk-based challenges, without disrupting genuine users.

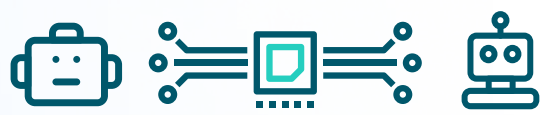
OVERVIEW

An Asia-based online marketplace handling millions of SKUs (Stock Keeping Units) and daily checkouts began seeing AI bots distort demand, scrape pricing and inventory, abuse promo flows, and probe account and payment endpoints. Leadership also wanted to reduce regulatory exposure following an incident in 2023 in which unauthorized access to registered-customer information was discovered after suspicious activity earlier that year.

Our engagement with the client began with detect-only POC baselining across search, product, cart, checkout, and account flows using VisitorTag (behavioral fingerprinting). Because IntelliFend operates at the edge, no SDKs or major code rewrites were required, and genuine customers experienced no added friction. AccuBot then produced policy recommendations (rate thresholds, step-up triggers, bot allow/deny), plus a WAF Rule Advisory reviewed with the client’s infra team.

Controls were phased in monitor → challenge → block within IntelliFend’s enforcement layer, with each change, along with its effects, documented in the Push Log to ensure auditability and enable rollback.

THE CHALLENGE: WHEN “TRAFFIC” ISN’T CUSTOMERS



By Chinese New Year promotions, phantom searches and cart-adds surged. Advanced scrapers harvested live prices and stock in real time, then undercut official listings on third-party channels, while inventory-locking scripts held items without buying—showing “sold out” to humans and depressing conversion. Much of this activity was directed not only at the website itself but also at the APIs powering search, cart, and mobile checkout, which were increasingly probed and abused by bots.

Parallel campaigns targeted login and loyalty with credential stuffing and account takeover (ATO), and checkout with stolen-card tests that later drove cancellations and chargebacks. During big drops, bot storms saturated origin capacity, slowing pages and intermittently degrading the customer experience.

IntelliFend

Platform stability improved: compute and bandwidth consumption fell 30–40%, queue delays halved, and uptime stayed at 99.9% even under fivefold traffic spikes. APIs powering cart and checkout stabilized, providing clean telemetry. Internal and third-party audits confirmed compliance, with Push Log offering full traceability. Customer trust and revenue strengthened.

HOW INTELLIFEND HELPED

1. Phantom Demand & Inventory Hoarding

Bots faked search and availability checks, and mass-held items to create artificial scarcity.

HOW INTELLIFEND HELPED

VisitorTag profiled session behavior (scroll/move cadence, request timing, fingerprint coherence) at IntelliFend's edge; AccuBot scoreda intent and applied adaptive rate-limits and step-ups to non-human patterns. That freed real inventory and stabilized demand signals.

2. Content Scraping & Price Undercutting

Headless browsers scraped prices/stock to feed comparison and grey-market listings.

HOW INTELLIFEND HELPED

Good-bot whitelists (major engines/partners) plus policy hooks to honor AI-use directives (e.g., IETF "AI Preferences" where implemented) allowed compliant automation while blocking unauthorized crawlers and high-risk sequences.

3. Account Takeover & Loyalty Abuse

Credential-stuffing waves targeted login; compromised accounts led to points theft and profile/PII exposure.

HOW INTELLIFEND HELPED

Risk-based challenges (MFA only on high-risk), device reputation, and path-aware heuristics (e.g., reset-email patterns) cut ATO success while keeping friction low for humans.

4. Checkout Fraud & Chargebacks

Stolen-card "tests" and scripted bookings inflated refunds, no-shows, and chargebacks.

HOW INTELLIFEND HELPED

Real-time risk signals from VisitorTag and AccuBot fed the payments pipeline; high-risk transactions were stepped-up or routed for extra verification, reducing post-auth losses.

5. Business-Logic Abuse & Promo Exploitation

Bots scripted rapid flash-sale claims, abused gift card loops, fake account creations, and loyalty rewards, all under the guise of normal traffic.

HOW INTELLIFEND HELPED

- Behavioral intelligence flagged logic-layer abuse patterns, even when headless and human-like and enforces dynamic throttling, step-ups, or policy blocks. This stopped underlying theft of value, not just the traffic.

6. Performance Degradation

Bot storms mimicked peak traffic, exhausting CPU, memory, and bandwidth, and triggering costly autoscaling.

HOW INTELLIFEND HELPED

- Upstream containment at IntelliFend's edge shed malicious volume before origin, shortening queues and improving page responsiveness through sales spikes.

7. API Protection in a Complex Retail Stack

Bots aggressively targeted APIs behind the storefront—cart, loyalty, and checkout endpoints—attempting enumeration, abuse of parameters, and scripted order loops.

HOW INTELLIFEND HELPED

- IntelliFend monitored behavior across both web and API layers, applying intent scoring and rate controls on API calls. VisitorTag fingerprints were tied to API sessions, ensuring continuity of human vs. bot classification across channels (web, mobile, partner integrations). This closed an often-overlooked vector for automated abuse.

8. Proof, Governance, and Ops

Security and Ops teams needed a reliable way to demonstrate control changes, review false positives, and fine-tune thresholds without hurting conversion. Manual notes and ad-hoc reporting made it hard to show auditors and compliance teams a full picture.

HOW INTELLIFEND HELPED

- Every policy change, anomaly, and mitigation action was automatically captured in Push Log, creating an exportable, audit-ready trail. Ops and Security teams could review weekly "drift" reports and false-positive deltas, then adjust thresholds in IntelliFend's dashboard with confidence.
- Importantly, these protections were enforced invisibly in the background—unlike CAPTCHA-heavy approaches—so customer conversion stayed intact and developers avoided heavy integration overhead.

IntelliFend

THE PAYOFF: PERFORMANCE, COMPLIANCE, AND TRUST RESTORED

The results of the rollout quickly became apparent. Instances of inventory-locking and scalper bots, once a persistent problem during major sales campaigns, fell to a negligible baseline. Real customers no longer encountered “sold out” notices when products were still available, a shift that was especially visible across two consecutive promotional cycles.

At the same time, the protection of customer accounts and loyalty balances improved measurably. Behavioral checks and risk-based step-ups reduced the success rate of credential-stuffing attempts and points-draining attacks by around 60-70% during the observation period. This was achieved with minimal friction for genuine users, who continued to log in and redeem offers without disruption.

The platform itself also became faster and more reliable. With scraper-driven requests contained at the edge, compute and bandwidth consumption fell by roughly 30-40%. Queueing delays were cut in half. Even under traffic surges up to five times normal levels, the platform maintained 99.9% uptime, ensuring a steadier experience during peak shopping windows. APIs powering cart, checkout, and loyalty flows also stabilized, with fewer anomalous request spikes and cleaner telemetry for the development team.

Finally, the solution enhanced compliance assurance. Both internal and independent third-party audits recorded no material findings related to payment-page script integrity or access controls. With IntelliFend’s Push Log providing a comprehensive record of every policy change and action taken, the retailer could deliver end-to-end evidence packs aligned to local data protection requirements and PCI DSS v4.0 expectations.

WHY THIS MATTERS AFTER THE 2023 INCIDENT

The company’s regulatory filing disclosure showed how quickly unauthorized access to customer information can occur and how sector-wide bot pressure magnifies operational and reputational risk. By shrinking automated exfiltration paths, enforcing behavior-based authentication, and documenting every mitigation, IntelliFend helps marketplaces like this client’s lower the likelihood and blast radius of web/API-layer data leaks while keeping the store fast and available.

IntelliFend

ABOUT INTELLIFEND

IntelliFend, a product of Innovenx, delivers advanced, cost-effective AI-powered bot management solutions with unparalleled accuracy. Our platform, driven by the AccuBot Detection Engine and unique VisitorTag tracking technology, leverages multi-layered analysis of both client-side and server-side signals to provide precise, real-time bot detection and mitigation. IntelliFend's sophisticated visitor-level analysis ensures more accurate identification of bot threats, helping businesses reduce false positives and improve overall security. Gaining trust from enterprises across various sectors, IntelliFend offers rapid deployment, seamless integration, and detailed analytics, delivering robust bot protection and operational efficiency.

CONTACT US

www.intellifend.com

support@intellifend.com

https://www.facebook.com/intellifend

https://www.linkedin.com/company/intellifend

https://www.youtube.com/@intellifend

20250924-EN