IntelliFend

CASE STUDY

How IntelliFend Fortifies Bot Defense for a Global Gaming Platform

Customer

A Leading Global Online Gaming Platform

Industry

Online Gaming / Esports

Challenge

Rising threats from bots during peak events (e.g., tournaments, in-game sales).

- **Credential stuffing:** Distributed brute-force login attempts.
- **Content scraping:** Real-time pricing theft and manipulation.
- **Automated betting:** Exploiting odds updates for unfair advantages.
- **System exploitation:** Hidden endpoint scanning and probing.
- **Others:** Degraded user experience, financial loss, and trust erosion.

Result

- 80% drop in account takeover attempts
- 60% reduction in scraper traffic and AWS bandwidth costs
- 5x traffic handling during esports tournaments without performance issues
- Enhanced visibility into bot traffic and login behavior via real-time telemetry

OVERVIEW

A leading global online gaming platform was struggling with increasing bot-driven threats, including account takeovers, credential stuffing, content scraping, and automated betting exploits. Despite deploying Web Application Firewalls (WAFs) and DDoS protection, these traditional tools fell short in distinguishing between legitimate users and bots, leading to fraud, resource drain, and degraded user experience. To counter these challenges, the gaming platform turned to IntelliFend. By leveraging machine learning, rule-based detection, and multi-layered security analysis, IntelliFend provided real-time threat detection, improved fraud prevention, and optimized operational efficiency.

THE CHALLENGE: GROWING BOT THREATS IN ONLINE GAMING

With millions of daily users, the gaming platform frequently saw traffic surges during major events, such as esports tournaments and in-game sales. However, this growth also attracted sophisticated bot attacks, which created severe security and business challenges:

1. Credential Stuffing & Account Takeovers (ATO)

Attackers used stolen credentials to perform brute-force login attempts on user accounts. The platform's WAF-based rate limiting was ineffective, as attackers rotated thousands of IP addresses to bypass restrictions.

HOW INTELLIFEND HELPED

- AccuBot Detection Engine grouped related login attempts across distributed IPs, identifying coordinated bot-driven account takeovers that bypassed traditional security rules.
- VisitorTag Tracking Technology ensured genuine human users were not mistakenly blocked, reducing false positives during login authentication.
- Machine learning models continuously analyzed login patterns, adapting in real-time to identify new attack strategies.

IntelliFend

2. Automated Scraping & Price Manipulation

The platform used real-time dynamic pricing for in-game items. Scraper bots targeted API endpoints and pricing data from specific URLs, allowing competitors to steal pricing data and adjust their own game pricing unfairly.

HOW INTELLIFEND HELPED

- VisitorTag analyzed browsing behaviors, distinguishing between real players and automated scrapers
- AccuBot assigned higher risk scores to suspicious traffic requesting bulk data extraction from pricing APIs, throttling bot requests without disrupting legitimate users.
- Rule-based detection flagged high-frequency API requests, automatically blocking excessive scraping behavior

3. Automated Betting Exploits

Bots exploited real-time odds changes in esports betting by placing bets within milliseconds of updates. This unfair advantage disrupted the platform's betting ecosystem, reducing fairness for human players.

HOW INTELLIFEND HELPED

- AccuBot's real-time risk scoring detected automated betting patterns, preventing bots from manipulating odds-based bets.
- VisitorTag ensured real human bettors experienced smooth gameplay without security interruptions.
- Machine learning identified abnormal betting behaviors, adapting to evolving bot tactics.

4. Web Scanning & Exploitation Attempts

Attackers targeted admin and configuration URLs to probe for security misconfigurations. Like port scanning, these attacks sought to identify weaknesses that could lead to data breaches.

HOW INTELLIFEND HELPED

- AccuBot flagged anomalous URL requests that deviated from normal user behavior, blocking web scans before attackers could exploit vulnerabilities.
- VisitorTag's telemetry tracking helped identify users repeatedly accessing suspicious admin endpoints, escalating their risk scores dynamically.
- Rule-based threat identification blocked requests to unauthorized paths, reducing security risks.

IntelliFend

DYNAMIC & RULE-BASED DETECTION FOR BOT DEFENSE

To effectively mitigate these threats, the gaming platform deployed IntelliFend's AccuBot and VisitorTag, creating a multi-layered defense against bot attacks.

1. VisitorTag: Behavioral Tracking for Human User Detection

- Analyzed user behaviors (mouse movements, scrolling speeds, tap delays) to separate human players from bots.
- Created unique device identifiers using hardware attributes and session telemetry, tracking repeat bot users even if they changed IPs.
- Prevented false positives, ensuring that legitimate players weren't accidentally blocked.

2. AccuBot: AI-Driven Risk Scoring & Real-Time Adaptation

- Processed real-time login and browsing data, detecting bot patterns across thousands of distributed IPs.
- Assigned risk scores to each session, throttling or blocking malicious traffic while allowing real players seamless access.
- Dynamically adapted to bot behavior, making it harder for attackers to bypass detection compared to WAF-based rule systems.

3. Hybrid Detection: Combining Machine Learning & Rule-Based Filtering

IntelliFend doesn't rely on a single factor to determine bot behavior. Instead, it employs:

- **Machine Learning**: Learns bot behaviors over time, improving detection accuracy.
- **Behavioral Analysis**: Tracks mouse movements, scrolling speeds, and tap frequencies.
- **IP Reputation & Risk Scoring**: Groups suspicious IP clusters, rather than relying on static blacklists.
- **Rule-Based Detection**: Instantly flags obvious bot behaviors, like headless browsers or abnormal session patterns.

4. Real-Time Data Streaming with Push Logs

- IntelliFend's push log feature enabled continuous traffic data streaming from the client's NGINX servers for real-time monitoring.
- The gaming platform used this data-driven intelligence to build a custom dashboard, extending visibility beyond bot detection.
- Through its custom-built dashboard, the client tracked login patterns, user segmentation, and bot activity trends over time.
- Instead of immediately blocking bots, the client leveraged AccuBot's risk scoring and VisitorTag's behavioral tracking to categorize different bot behaviors.

IntelliFend

THE RESULTS: STRENGTHENED SECURITY, REDUCED COSTS, AND IMPROVED UX

Following the IntelliFend deployment, the gaming platform saw dramatic improvements in security, efficiency, and cost savings:

1. 80% Reduction in Account Takeover Attempts

- AccuBot blocked over 7 million bot-driven logins daily, preventing credential stuffing attacks.
- Adaptive machine learning continuously refined detection, making it harder for attackers to adapt.

2. 60% Reduction in Scraper Traffic & Bandwidth Costs

- VisitorTag eliminated unauthorized scraping, reducing bandwidth consumption and AWS costs.
- Rule-based filters automatically throttled excessive API requests, minimizing system strain.

3. Scalable Security for High-Traffic Events

- Auto-scaling Kubernetes clusters ensured that bot detection remained fast and efficient during high-demand gaming events.
- IntelliFend handled 5x more traffic without impacting performance.

WHY INTELLIFEND?

Unlike traditional WAF-based security, IntelliFend's AccuBot & VisitorTag provided:

- AI-Powered Behavioral Tracking: Accurately distinguished bots from real users using multi-layered telemetry data.
- Hybrid Detection Approach: Combined machine learning with rule-based filtering for adaptive bot defense.
- Scalable API Integration: Provided customizable security solutions, giving the company full control over bot management.

INTELLIFEND FOR GAMING & BEYOND

While this case study exemplifies IntelliFend's success in the gaming industry, its AI-driven, behavior-based bot detection is equally effective for:

E-Commerce & Retail
Preventing scalping & fake account creation

Financial Services
Protecting against credential stuffing & automated fraud

Travel & Ticketing
Blocking bots from hoarding airline tickets & event passes

Media & Digital Publishing
Stopping content scraping & ad fraud

With bots evolving rapidly, relying solely on WAFs and rate-limiting falls short. IntelliFend's AI-driven bot management provides long-term protection, ensuring security, cost-efficiency, and platform stability across industries.

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

20250404-EN