DataVisor Enables Top Online Marketplace to Defeat Mass Registrations and Fake Listings

CLIENT A global online marketplace operating in 40+ countries with over 350 million monthly active users.

CHALLENGE The client was plagued by mass-registered accounts that would first incubate for weeks, then start launching fake listings to scam good users. The accounts were highly coordinated and shared similar patterns, but the client's current solutions could only capture a portion of the fraud rings due to an inability to identify the cross-account linkages among all of the accounts. The solutions were also not able to analyze unstructured data and metadata and therefore could not reliably detect large-scale fake listings.

RESULTS

of fraudulent accounts caught before the first scam

Auto-action on over 65% of detections

68k+

accounts caught in the largest fraud ring

>20%

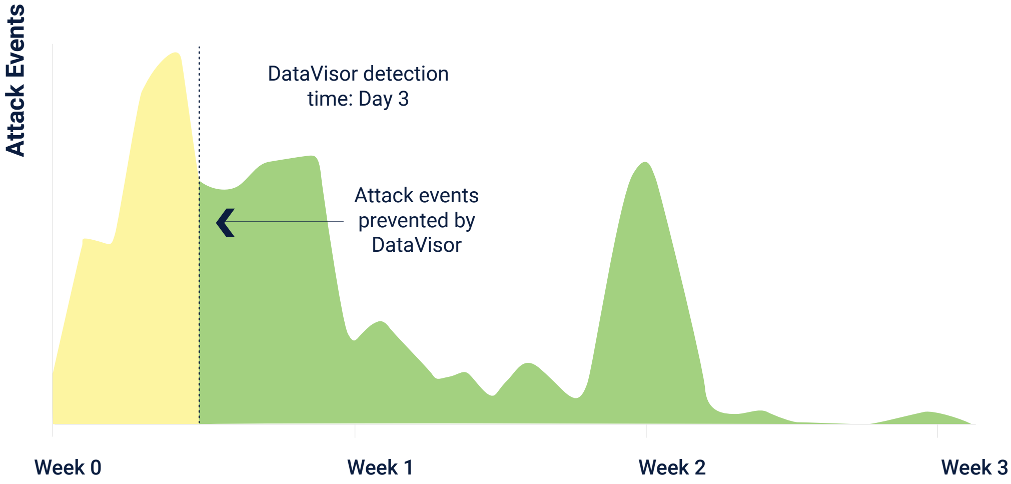
detection accuracy improvement over existing solutions

FRAUD PATTERNS DETECTED

- Disposable emails for registrations; bots for scripted logins from cloud hosting IPs
- 2-minutes intervals between login and attack; similar listing descriptions created from templates with shared URLs
- “Hit-and-run” behavior: 60% of fraudulent accounts made the first attack within 2 hours of registration; 76% made the first attack within 24 hours of registration
- Sleeper cells: some accounts logged in then remained dormant for weeks prior to a large-scale scam
- Human-operated scam farms: a group of scam armies was highly correlated on behavioral patterns such as event sequences, event time, and intervals. They attacked weekdays and rested on public holidays and weekends

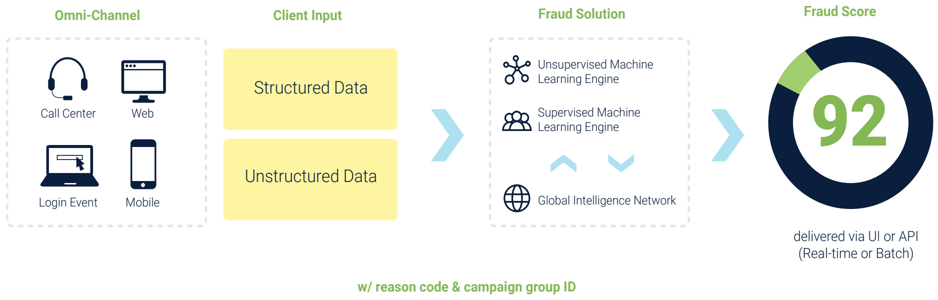
HOW DATAVISOR HELPED

DataVisor's solutions uncovered suspicious accounts and coordinated fraudulent registrations early in the incubation stage, and flagged scam content by analyzing posts and images and spotting similar attributes and behaviors across accounts.



HOW DATAVISOR DETECTION WORKS

The DataVisor approach enables proactive fraud protection. While conventional rules or model-based solutions require “pre-knowledge” of how attacks work to be effective, DataVisor’s systems are architected to detect fraud attacks without any historic labels, large datasets, or training time. Drawing on a proprietary UML engine, DataVisor’s solutions accelerate detection by analyzing all accounts and events simultaneously and identifying suspicious clusters of malicious activity—even at the point of account registration. This approach is ideal for finding new and unknown attacks because it does not require historical data and constant retuning.


Omni-Channel
Call Center
Web
Login Event
Mobile
Client Input
Structured Data
Unstructured Data
Fraud Solution
Unsupervised Machine Learning Engine
Supervised Machine Learning Engine
Global Intelligence Network
Fraud Score
92
delivered via UI or API (Real-time or Batch)
w/ reason code & campaign group ID

To enhance detection efforts and enrich decision-making, DataVisor also leverages its Global Intelligence Network (GIN), which is comprised of anonymized non-PII data from over 4 billion protected accounts and 800 billion events across the globe. The GIN contains rich information on digital data such as IP address subnets, prefixes, proxies and data centers, user agent strings, device types and OS, email address domains, and more. Information from the GIN feeds into machine learning algorithms to further improve overall detection.

CONTACT US

If you are interested in learning how DataVisor can help bring your fraud detection to the next level or wish to start a trial to assess your current fraud exposure level, please contact us at: **info@datavisor.com** or visit us at **www.datavisor.com**

DATAVISOR

967 N. Shoreline Blvd.
Mountain View | CA 94043