Data Contamination Defense

Prevent fake interactions and ensure accurate analytics

Data Contamination Defense

Data Contamination Defense blocks automated website engagements and fake form fills, optimizes resources, filters out bot traffic from your data. The solution uses advanced machine learning, behavioral analysis, and intelligent fingerprinting to identify bots on web and mobile applications and APIs. It then delivers optimal bot management, including hard blocks, honeypots, and misdirection. Known bots and crawlers are allowed to proceed unimpeded, and bots can be shown alternative content and pricing if desired.

Data Contamination Defense is part of Application Protection, a suite of solutions purpose-built to secure web and mobile applications from a range of cyberthreats.

What We Defend Against

- **FAKE LIKES AND SOCIAL INTERACTIONS**
- **SPAM COMMENTS AND REVIEWS**
- **FAKE FORM FILLS**
- **ROYALTY FRAUD**
- **SKEWED ANALYTICS**

"We can trust our data and analytics with HUMAN's bot mitigation solution. With HUMAN, you just set it and forget it – and have peace of mind."

VP OF E-COMMERCE
at Samsonite

Samsonite

Benefits

PROTECT DATA-DRIVEN DECISIONS

Remove bot traffic from your website metrics, so you can have confidence in your reporting

PRESERVE USER TRUST

Block fake likes, reviews, comments, and form fills, so only real humans interact with your application

OPTIMIZE RESOURCES

Reduce bandwidth strain and wasted spend, and save time manually responding to bots

HOW IT WORKS

COLLECTS
hundreds of non-PII client-side indicators

DETECTS
human vs. bot activity using machine learning models

MITIGATES
bot traffic according to customizable threat response policies

REPORTS
incident details in intuitive dashboards for easy investigation and analysis

OPTIMIZES
detections by continuously updating ML models with relevant data

Key Capabilities

Seamless integrations. Integrate with leading analytics platforms, including Google Analytics and Adobe Analytics

HUMAN Sightline. Automatically isolate distinct bot profiles and reveal in granular detail what each attacker is doing on your application.

Data export. Easily export your metrics and logs to Datadog, Splunk, Amazon S3, and other platforms

Secondary detection. Uncover hidden threat patterns by automatically analyzing all current and historical traffic data in aggregate after an initial

Precheck and Human Challenge. Low-friction, scenario-optimized challenges block bots at the edge, before they can access a single page.

Adaptive learning. AI models spot nuanced bot behavior shifts and automatically optimize mitigation workflows.

The Human Advantage

Scale
We verify more than 20 trillion digital interactions weekly across 3 billion unique devices providing unrivaled threat telemetry.

Speed
Our Decision Engine examines 2,500+ signals per interaction, connecting disparate data to detect anomalies in mere milliseconds.

Decision Precision
Signals from across the customer journey are analyzed by 400+ algorithms and adaptive machine-learning models to enable high-fidelity decisioning.

HUMAN is a leading cybersecurity company committed to protecting the integrity of the digital world. We ensure that every digital interaction, transaction, and connection is authentic, secure, and human. HUMAN verifies 20 trillion digital interactions, providing unparalleled telemetry data to enable rapid, effective responses to the most sophisticated threats. Recognized by our customers as a G2 Leader, HUMAN continues to set the standard in cybersecurity. For more information, visit ***www.humansecurity.com***