HUMAN

Account Takeover Defense

Secure online accounts against automated account takeover attacks

Account Takeover Defense

Account Takeover Defense stops automated account takeover attacks by blocking mass credential stuffing and cracking attempts and neutralizing stolen or breached credentials. Sophisticated bots are caught at the account perimeter and advanced threat intelligence analyzes compromised credentials from the latest data breaches and attacks. It enables security professionals to spend less time investigating account takeover attacks and more time focusing on other mission critical tasks.

Account Takeover Defense is part of both Account Protection and Application Protection, a suite of solutions purpose-built to secure online accounts, websites and applications from a range of cyberthreats.

What We Protect Against

- THEFT OF STORED VALUE/ACCOUNT BALANCE
- ILLICIT CREDIT CARD USE
- FRAUDULENT CREDIT APPLICATIONS
- DEPLOYMENT OF PHISHING EMAILS
- TARGETED INFORMATION THEFT (PII)
- INFRASTRUCTURE COSTS

> **"We seamlessly integrated HUMAN at our platform edge [AWS CloudFront] to ensure maximum protection against automated bot attacks, but also to minimize latency."**
>
> ***SENIOR DIRECTOR, ARCHITECTURE*** *AT FANDUEL*
>
> FANDUEL

Benefits

PROTECT ACCOUNT AUTHENTICATION

Block automated credential stuffing and bruteforcing attacks from bypassing the login process.

STAY AHEAD OF ATTACKERS

Render compromised account credentials useless before cyber-criminals use them in an attack.

MINIMIZE THE COST OF AN ATTACK

Automatically neutralize attempted attacks and spend less time investigating incidents.

How It Works

COLLECTS

non-PII indicators to determine human vs bot activity and compromised credentials

DETECTS

normal range for human activity with ML and attempts to use compromised credentials

INTERVENES

to block unwanted bot traffic and login attempts with compromised credentials

REPORTS

key incident data that is easy to understand, investigate and share

Key Capabilities

Advanced detections based on behavioral analysis, intelligent fingerprinting, predictive models, and 400+ algorithms

Mitigation responses via customer-specific policies to serve hard blocks, honeypots, misdirection, and alternative content

Compromised credentials intelligence using a proprietary, dynamic collection of stolen credentials to stop compromised login attempts

Login dashboard shows all traffic to login pages including blocked and legitimate traffic, top incident types, top domains and top blocked IPs

Analyzer dashboard speeds investigation, such as understanding why an IP was blocked, which pages it was targeting, and header referrers

Single pane of glass management: Manage all your HUMAN solutions from one console. It's easy to see key details, edit policies, and share data

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***