HUMAN

HUMAN Credential Intelligence

Early Warning System to Prevent Account Takeover

Security, fraud, risk, compliance and engineering teams spend significant resources combating account takeover (ATO) and credential stuffing attacks. The majority of these attacks use compromised credentials—usernames, email addresses, and matching passwords—acquired from a data breach or purchased on the dark web. When validated in a credential stuffing attack, they become valuable to cybercriminals, enabling them to gain unauthorized access to legitimate user accounts. With these credentials, attackers can transfer funds, use stored credit cards, deplete gift cards and loyalty points, redeem airline miles, and submit fraudulent credit applications. Widespread attacks on customer accounts can cause considerable damage to the brand, both in the short term and in the longer term, including: harming brand reputation, disrupting consumers' digital experience, increasing churn and regulatory fines.

HUMAN Credential Intelligence

HUMAN Credential Intelligence is a cloud-native web application security solution that detects and stops the use of compromised credentials on websites and mobile apps in real-time. The power of Credential Intelligence is the dynamic, and up-to-date collection of compromised credentials that HUMAN builds from its position safeguarding some of the most popular and highly trafficked sites on the web. With this solution organizations may take mitigating action when a known compromised credential is attempted to be used before any damage is done.

Credential Intelligence stops the use of stolen credentials, decreasing fraud claims and saving money in the form of lower transaction fees and fewer write-offs. The solution also helps businesses provide additional value to their consumers and account holders by ensuring accounts cannot be taken over by a bot or threat actor, improving customer satisfaction and protecting brand reputation.

Ensure Customer Accounts are Safe

By detecting and preventing the use of compromised credentials before an ATO takes place, HUMAN ends the business threat of credential stuffing attacks. Further, the solution provides a strong disincentive for future attacks. And once HUMAN identifies a credential stuffing attack for one customer, all customers benefit from this intelligence.

"We've seen a significant improvement in our ability to proactively prevent attacks which really takes the pressure off our team. Customer complaints have also decreased now that accounts are secure and we no longer have outages due to spikes in credential stuffing attempts."

Principal Product Security Engineer at a Global E-Commerce Retailer

Benefits for digital businesses

Protect Your Most Loyal and Vulnerable Customers

Build brand loyalty, protect customers' most valuable assets and identity, reduce social media exposure.

Reduce Risk and Preserve Your Brand Reputation

Maintain your brand reputation, eradicate the cycle of credential stuffing on your site and increase your customers' confidence and trust.

Improve Operational Efficiency

Reduce customer complaints and support calls associated with password resets and refund requests, avoid write-offs and chargebacks and defend against regulatory fines.

How it Works

COLLECT
A real-time collection of credentials harvested from global and targeted attacks.

DETECT
An account that is attempted to be accessed using credentials is flagged as compromised in real-time.

MITIGATE
Use the signals to block ATO attempts before any damage is done. Implement automated playbooks or integrate with the CIAM provider.

LEARN
Constant collection of credentials from the entire network to improve fraud detection.

The HUMAN Advantage: Better Together

Credential Intelligence harnesses the power of HUMAN Bot Defender® to offer an additional layer of defense to stop the use of breached credentials on your website or mobile app. Bot Defender blocks credential stuffing attacks, thus blocking potential ATO. However, blocking credential stuffing attacks does not stop threat actors from future attempts; the same list of credentials is still as relevant as before they were stopped on a site protected by HUMAN. Credential Intelligence flips the script on the basic economic viability of credential stuffing attacks by making the lists of compromised credentials irrelevant and useless in the future for any sites it protects. Furthermore, because the collection contains information that HUMAN brings together from multiple customers, once intelligence on attacks is gathered for one customer, all customers get the benefit.

Powered by Human Defense Platform

HUMAN uses a modern defense strategy to safeguard organizations from credential based attacks and fraud, increasing ROI and trust while decreasing customer friction, data contamination, and cybersecurity exposure. Credential Intelligence runs on the HUMAN Defense Platform, which powers an award-winning suite of application protection solutions enabling full visibility and control to understand when a compromised credential is in use and take action to stop the threat.

Key Integrations

Edge Integrations (CDN, Cloud)

fastly · YOTTAA · CLOUDFLARE · amazon cloudfront · Akamai

Application SDK/Middleware

node · Java · Ruby · GO · python

Load Balancers and Web Servers

APACHE · NGINX · citrix NetScaler · f5

Serverless and Cloud Frameworks

E-commerce Platforms

salesforce commerce cloud · Magento

About HUMAN

HUMAN is a cybersecurity company that safeguards 500+ customers from sophisticated bot attacks, fraud and account abuse. We leverage modern defense—internet visibility, network effect, and disruptions—to enable our customers to increase ROI and trust while decreasing end-user friction, data contamination, and cybersecurity exposure. Today we verify the humanity of more than 15 trillion interactions per week across advertising, marketing, ecommerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN. **To Know Who's Real, visit www.humansecurity.com.**