Case Study

Global Leader in Business Data and Analytical Insights Protects Against Credential Breaches and Satisfies NIST Compliance

Company

Global data and analytics entity possesses high-value data post-login. Their intellectual property and aggregated data is accessed by millions of global users on a regular basis. As a result, their logins require extra rigor with regard to credential breaches and account takeover.

Challenge

This global data and analytics company holds high-value data in user accounts. Because users can access such sensitive information post-login, the company needed to take extra precautions to prevent credential breaches and account takeover. In addition, the company is using an Identity and Access Management (IAM) platform that does not satisfy NIST 800 63B requirements, in particular section 5.1.1.2.

In order to comply with NIST, the company was faced with either implementing further controls that would add extra complexity for their operations team or switching IAM providers—neither of which was an ideal solution. They needed a real-time, in-line solution for finding compromised credentials that would ensure compliance without requiring code integration with their IAM.

> **"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

Solution

The company implemented HUMAN Account Protection, a cloud-native web application security solution that quickly finds and stops the use of compromised credentials on websites and mobile apps. It is powered by a proprietary collection of expansive, dynamic and up-to-date information that HUMAN gathers from its globally deployed sensors. The solution provides early signals when cybercriminals are attempting to use stolen credentials on their site, so preemptive mitigating action can be taken. Additionally, it can warn users that their credentials have been breached and trigger a password reset.

DATA BREACHES

ACCOUNT TAKEOVER

CREDENTIAL STUFFING

WEB SCRAPING

PII HARVESTING

NIST 800-63B

Results

With Account Protection, the company was able to satisfy NIST 800-63B requirements without disrupting their existing IAM solution. This added defense-in-depth with the following benefits:

- **Login protection** for their users to prevent account takeover and stolen PII
- **Protect intellectual property** and high-value data from scraping
- **Preserve reputation** and reduce risk
- **Continuous validation** against stolen credentials through network effect
- **Operational efficiency** through reduction of account compromise, etc
- **Compliance with NIST** 800-63B, Section 5.1.1.2 requirements
- **No disruption** to current technology stack

About HUMAN

HUMAN is trusted by the world's leading enterprises and internet platforms to prevent, detect, and respond to cyber attacks with unmatched scale, speed, and decision precision across their advertising, application, and account surfaces. Safeguard your customer journey end to end with complete confidence by consolidating with the Human Defense Platform.