

## HUMAN Sightline Cyberfraud Defense 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 Sightline](#), 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 HUMAN Sightline, 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
- **Compliance with NIST 800-63B**, Section 5.1.1.2 requirements
- **No disruption** to current technology stack

## About HUMAN

*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](http://www.humansecurity.com)*