HUMAN

Application Protection Case Study

Online Learning Company Protects Against Carding and Digital Skimming

This online learning company is a leading education technology innovator, creating engaging and effective learning resources to help children build a strong foundation for academic success. Its flagship product in the United States is a comprehensive curriculum for preschool through second grade, available on all major digital platforms and used by tens of millions of children.

> **"Application Protection is a very vital piece of our security posture. Now, we can maintain CCPA and GDPR compliance. And we can manage where our data is going and what is being collected."**
>
> — Director of Information Security, Online Learning Company

Challenge

The COVID-19 pandemic spurred exponential growth in virtual education, raising the online learning company's popularity—and making it a bigger target for bot attacks. The company's security team noticed an increase in carding attacks on its websites, which led to financial losses from chargebacks and damaged consumer trust. The high volume of bot traffic also skewed the company's web analytics and required hours of manual work to clean up.

Additionally, the online learning company relied on third-party JavaScript and open-source libraries to build its websites. They realized that some of this JavaScript could access users' PII when they typed it into site forms, a data privacy compliance violation. They needed full visibility and control of third-party script behavior to ensure compliance and prevent digital skimming attacks.

Solution

The online learning company wanted a single platform to address bot attacks and client-side threats. HUMAN Application Protection met their needs on both fronts.

TRANSACTION ABUSE DEFENSE AND DATA CONTAMINATION DEFENSE

- Uses machine learning algorithms, behavioral analysis, and predictive methods to accurately detect and mitigate carding and other bot attacks on web and mobile apps and APIs
- Filters out bot traffic from human traffic, so teams can use accurate data to inform their decisions
- Improves operational efficiency, freeing security teams to work on more strategic tasks

CLIENT-SIDE DEFENSE

- Detects anomalies in the behavior of first-, third- and nth-party scripts, such as unauthorized PII access and data exfiltration events
- Provides granular control to block specific actions a script is taking, so you can proactively mitigate potential data breaches and stop legitimate scripts from accessing sensitive data while otherwise letting them run as intended
- Simplifies compliance with standards and regulations, including PCI DSS 4 and GDPR

Application Protection use the same open architecture, making them easy to integrate with the company's existing infrastructure, including AWS CloudFront. Together, the solutions provide a layered defense model that protects against a range of cyberthreats.

Results

Application Protection has **protected an average of 26.5 million page views from bots** each month. The drop in malicious bot activity has saved the online learning company tens of thousands of dollars in chargebacks. Because Application Protection automatically removes bot traffic from website data, the company's marketing team has **saved almost 100 hours** each month manually sorting through metrics.

In addition, Application Protection **identified 562 scripts from 28 different source domains** that sent data to 74 destination domains. The solution discovered that the online learning company risked violating GDPR and CCPA because two of their legitimate third-party vendor scripts could access users' PII. Application Protection blocked access to the sensitive fields, helping ensure compliance.

All in all, the online learning company has gained real-time visibility and control into its client-side supply chain attack surface and remains protected from malicious bot attacks.

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***