perimeterx | Case Study

Top 5 Global Airline

Safeguards Customer Data Against Client-side Data Breaches

Company

This top 5 global airline is one of the largest airlines in the world offering scheduled passenger and cargo services to over 200 destinations in Asia, North America, Australia, Europe and Africa, carrying over 30 million passengers annually.

Problem

The airline was concerned about the risk to their business from potential Magecart attacks and wanted to protect their website from client-side data breaches. With 82% of all travel bookings happening online, protecting the airline's digital presence was a top priority for its executives.

Digital skimming and Magecart attacks have targeted several airlines recently including British Airways, Delta Airlines and easyJet. Airlines are a popular target because of the high volume of online transactions. These attacks resulted in client-side data breaches that not only hurt the companies' brand reputation but also resulted in compliance penalties and lawsuits. British Airways, for example, was fined $230 million by UK regulators for the data breach resulting from the digital skimming attack it suffered in 2018.

In order to innovate faster, the top 5 global airline's web application teams made extensive use of open source libraries and third-party code. The airline was concerned about the Shadow Code introduced through this digital supply chain. This increased the attack surface and could enable hackers to inject malicious scripts into the application. These scripts could then skim sensitive information from the website including credit card numbers, CVV codes and passwords potentially causing massive client-side data breaches.

> "The solution pays for itself by reducing our risk from client-side data breaches and helping us avoid fines and the subsequent negative impact to our brand reputation."
>
> **CISO**, Top 5 Global Airline

Solution

The airline examined multiple approaches and solutions to address this challenge. They realized that static scanning alone would be ineffective in finding and stopping client-side attacks, while a content security policy (CSP) solution would be too complex to manage. They needed a real-time client-side security solution that

could detect risks in first-, third- and Nth-party code across all web applications in use by the airline's customers as well as by its staff and booking agents.

After evaluating multiple solutions, the airline selected and deployed PerimeterX Code Defender, which provided the client-side protection they needed while preserving the website architecture, performance and user experience. Code Defender is a client-side application security solution that continuously protects websites from digital skimming, formjacking and Magecart attacks, preventing data breaches and reducing the risk of non-compliance.

Easy to deploy and integrate: The airline was able to easily integrate Code Defender by adding the PerimeterX JavaScript Sensor to their page template. They did not have to modify their website architecture or content delivery networks.

Behavior-based learning: Code Defender continuously collects signals from the client side and identifies behavioral anomalies such as scripts loaded from a new domain, modifications to the page, scripts accessing sensitive input fields, communication with malicious domains and known vulnerabilities in third-party scripts. These anomalies trigger prioritized incidents that are sent to the airline's monitoring systems.

No impact to user experience: The Sensor runs asynchronously on the web page and preserves the user experience. The application development teams at the airline are able to continue innovating with confidence while the information security teams have full visibility into the entire supply chain of website scripts.

Results

Code Defender helped the airline safeguard customer data by gaining continuous protection against client-side data breaches. It was able to reduce the risk of non-compliance, protect its brand reputation and ensure customer confidence.

Reduced risk of data breaches and non-compliance: Using Code Defender, the airline has continuous visibility and protection against client-side data breaches. This helps it ensure compliance with global data privacy regulations such as GDPR and CCPA, and reduce its business exposure to penalties and lawsuits.

Improved operational efficiencies: The airline realized significant operational efficiencies by eliminating the manual analysis of website scripts and third-party risks. It was also able to streamline operations by making security an enabler rather than a bottleneck in its application development process.

About PerimeterX

PerimeterX is the leading provider of application security solutions that keep your business safe in the digital world. Delivered as a service, the company's Bot Defender, Code Defender, and Page Defender solutions detect risks to your web applications and proactively manage them, freeing you to focus on growth and innovation. The world's largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers' digital experience. PerimeterX is headquartered in San Mateo, California and at www.perimeterx.com.

perimeterx

www.perimeterx.com