CASE STUDY

Enhancing Web Security for a Logistics Company

COMPANY OVERVIEW

A leading logistics company recognized the urgent need for a robust monitoring tool to ensure the security of their online payment and login pages. Due to the sensitive nature of the data handled on these pages, protecting them against cyber threats was paramount. Implementing a layered defense strategy was essential to safeguard customer information and maintain trust.

CHALLENGES

1

Rise of Magecart Attacks

The company's payment and login pages were prime targets for cybercriminals looking to exploit vulnerabilities through Magecart attacks.

2

Need for Constant Monitoring

Existing security measures, including a web application firewall (WAF), were not equipped to provide real-time detection and response to such threats.

3

Maintaining Customer Trust

Ensuring the safety of customer data was paramount to maintaining trust and avoiding reputational damage.

THE SOLUTION: WEBORION® MONITOR AND RESTORER

The logistics company implemented WebOrion® Monitor and Restorer, which complemented their existing WAF, enhancing the company's overall security posture.

▶ 24/7 Monitoring and Alerts

WebOrion® Monitor continuously scans web pages for suspicious activity and malicious code injections, and sends an alert if such hacks are detected,

▶ WebOrion® Monitor's JavaScript Malware Detection Engine

With the ability to detect malicious content, including cryptojacking and card-skimming scripts, the company will be informed if known malicious scripts are found. This allows IT teams to respond quickly to threats.

▶ One-click Restoration Solution

WebOrion® Monitor can be seamlessly integrated with WebOrion® Restorer, to allow a one-click failover to a temporary Secure Replica.

RESULTS

1

Comprehensive Coverage

By combining their existing web application firewall with WebOrion® Monitor, the logistics company significantly reduced the risk and impact of Magecart attacks. The WAF provided an essential first line of defense by blocking known threats and filtering malicious traffic, while WebOrion® Monitor continuously scanned for and identified sophisticated threats that managed to bypass the WAF.

2

Improved Customer Confidence

The logistics company's commitment to securing its online payment and login pages through a multi-layered defense strategy greatly enhanced customer trust. Customers felt reassured knowing that their sensitive information was protected by robust security measures, maintaining the company's reputation and fostering long-term customer loyalty.

CONCLUSION

By leveraging a layered defense approach, the logistics company successfully mitigated the risk of cyber threats, ensuring the security of its critical online pages. This comprehensive security strategy highlights the effectiveness of combining multiple security solutions to protect sensitive data and maintain operational integrity in the digital age.