wallarm

Manufacturer Defends Against API Attacks with Wallarm API Security

Stronger defenses and simplified deployment with Wallarm

CASE STUDY

MANUFACTURING

wallarm

Modern Design and Manfuacturing

This organization designs, manufactures and repairs some of the most complex and innovative optical, electronic and mechanical products in the world. Recognized as a technology leader, the organization provides end-to-end design, manufacturing and logistics solutions, delivering superior quality and support to Original Equipment Manufacturers (OEMs) primarily in the industrial, medical, defense and aerospace, automotive, communications networks and cloud solutions sectors.

Publicly traded, more than **40 years old** and **$8B** in annual revenue

Approximately **35,000 employees** in **20** countries on 6 continents

Fortune 500 Company

Known for printed circuit boards, but serves industries such as communications networks, cloud solutions, industrial, medical, automotive, and defense & aerospace

Overview

Faced with increasing API security challenges, including an API security incident and insufficient static code analysis, this manufacturer sought a robust solution to protect its APIs. After evaluating several vendors, they chose Wallarm for its ease of use, low false-positive rates, and competitive pricing. Since implementation, Wallarm has significantly enhanced their API security posture by reducing malicious traffic, improving threat detection, and streamlining deployment. Exceptional customer support and advanced features like credential stuffing protection have solidified Wallarm as an integral part of their security strategy.

Challenges

Before implementing Wallarm, the organization grappled with several API security challenges:

Insufficient Security Measures

Relying on Imperva with no API security capabilities left critical gaps in their defenses. Previous evaluations of the available API Security add-on from Imperva were unsatisfactory, and existing static code analysis processes proved inadequate, missing key vulnerabilities.

Security Incident Exposure

An API security breach underscored their vulnerability and highlighted the need for a more robust, proactive approach to API protection.

Developer-Driven Risks

As developers created APIs, the reliance on static analysis tools alone was insufficient to detect all potential threats, leaving the organization exposed to missed vulnerabilities.

These challenges not only put the organization at risk but also disrupted operations and prompted a reevaluation of their API security strategy.

wallarm

Solution

The organization chose Wallarm after evaluating several leading API security solutions, including Imperva and Traceable. Their decision was driven by Wallarm's unique combination of effectiveness, ease of use, and cost efficiency.

Ease of Deployment

Unlike competitors, Wallarm required minimal tuning to deploy effectively, saving time and reducing operational overhead. Traceable and Imperva, by contrast, demanded extensive configuration to function optimally.

Accurate Threat Detection

Wallarm's low false-positive rate ensured accurate identification of malicious traffic, enhancing the team's confidence in their security tools.

Competitive Pricing

With pricing more accessible than alternatives, Wallarm offered an affordable yet comprehensive API security solution.

Wallarm successfully addressed the organization's API security challenges:

Enhanced Protection

Wallarm's advanced triggers and brute force detection capabilities blocked malicious traffic before it could impact internal applications.

Operational Improvements

By reducing the load on protected applications, Wallarm increased system reliability, as evidenced during a recent penetration test where unprotected systems failed under attack.

Credential Stuffing Mitigation

Wallarm helped enforce stricter password policies, addressing vulnerabilities in applications with local logins.

Wallarm effectively solved the organization's critical security challenges, significantly improving their overall security posture.

wallarm

Outcomes

Implementing Wallarm delivered measurable improvements in the organization's API security and overall operational efficiency. By blocking malicious traffic at the edge, Wallarm reduced the load on internal applications, preventing disruptions and enhancing system reliability. New triggers, such as brute force detection, enabled proactive defense mechanisms that were previously unavailable, significantly improving threat mitigation. Wallarm's credential stuffing protections addressed key vulnerabilities, prompting stricter password policies and enhancing compliance. During a recent penetration test, the value of Wallarm's protection became evident when unprotected systems experienced downtime, while Wallarm-secured applications remained stable. The organization has seen clear benefits from Wallarm's solution, driving greater confidence in their API security strategy.

wallarm

BOOK A DEMO

www.wallarm.com
(415) 940-7077
188 King St. Unit 508, San Francisco, CA 94107