wallarm

Wallarm Delivers Governance and Performance at Scale for Enterprise SaaS Provider

Scaling API Security for a Data-Driven Enterprise

CASE STUDY

ENTERPRISE SAAS

wallarm

Enterprise SaaS at Enterprise Scale

This technology team within this enterprise SaaS provider ensures the company's technology infrastructure runs smoothly and efficiently. They work with cutting-edge technology to support cross-functional teams and develop solutions that transform the business. This team is responsible for everything from developing scalable internal applications to providing technical support and managing mission-critical business processes

This **$30B+ organization** employs more than **70,000 people** and serves more than **150,000** businesses worldwide.

The organization is pioneering the adoption of **Artificial Intelligence**, from AI applications to fully autonomous AI agents.

The organization offers a comprehensive suite of APIs, including **REST, SOAP, Bulk,** and **Streaming APIs**, which allow developers to integrate with other systems and build custom applications.

Overview

Faced with the challenge of securing thousands of APIs comprising tens of thousands of endpoints across a highly segmented architecture, this enterprise SaaS provider sought a comprehensive API security solution that could scale to one of the largest technology organizations in the world. With sensitive data flowing through rapidly developed APIs and manual security processes struggling to keep pace, the Enterprise Security team turned to Wallarm. After evaluating eight leading solutions, Wallarm stood out for its compatibility with MuleSoft and Heroku, robust API discovery features, and ability to manage data governance in hybrid deployments.

wallarm

Challenges

The organization faced a series of interconnected challenges:

Rapid API Development

APIs for internal use were being created and released at an accelerated pace, often without proper security measures in place.

Sensitive Data Exposure

These APIs contained critical organizational data, including financial, HR, and personal information, making them high-value targets.

Scalability

With over 1,500 APIs and more than 10,000 endpoints, securing this infrastructure required a solution that could scale without impacting performance.

Inefficient Security Processes

Manual reviews and penetration tests by the Enterprise Security team couldn't keep up with the speed of API development, leading to potential security gaps.

Data Governance Concerns

Many available solutions violated the organization's data subprocessor policies by requiring raw data to be sent to the cloud.

These challenges created a critical need for a solution that combined scalability, governance, and integration with existing infrastructure.

wallarm

Solution

The Enterprise Security team conducted an extensive evaluation of eight leading API security solutions, ultimately selecting Wallarm for its superior performance and unique features:

Data Governance

Wallarm's hybrid deployment approach allowed the organization to control the data between on-premise and cloud nodes, ensuring compliance with data subprocessor policies.

Scalability and Performance

Wallarm excelled in detecting attacks and minimizing false positives, even across a high-traffic API environment.

API Discovery and Monitoring

Real-time API discovery capabilities enabled the organization to map and secure APIs rapidly, identifying new endpoints as they were created.

Compatibility

Seamless integration with MuleSoft and Heroku ensured the solution fit into the organization's existing architecture without disruption.

Cost-Effective

Wallarm offered a competitive pricing model, balancing robust capabilities with affordability.

These features addressed the organization's need for a scalable, compliant, and high-performing API security solution.

Outcomes

Implementing Wallarm provided measurable improvements in API security and operational efficiency:

Faster Security Processes

Automated API discovery and attack detection significantly reduced the turnaround time for securing new APIs, aligning security processes with development cycles.

Improved Compliance

Wallarm's hybrid data governance capabilities ensured sensitive data remained secure and compliant with organizational policies.

Enhanced API Visibility

Wallarm's discovery features gave the Enterprise Security team unparalleled insight into the organization's sprawling API landscape.

Reduced Risk

Robust threat detection and false-positive minimization provided confidence in the security of APIs handling critical organizational data.

By aligning security capabilities with development demands, Wallarm empowered the organization to secure its API ecosystem while maintaining rapid innovation.

wallarm

BOOK A DEMO

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