

Wallarm API Protection for MuleSoft Anypoint Platform

Automated, Enterprise Grade API Security



APIs power modern software innovation, bridging systems for data and service access. However, this increased API use exposes vulnerabilities, attracting cybercriminals. Wallarm, a top cloud-based API security platform, defends against OWASP Top-10 vulnerabilities and more. The MuleSoft Anypoint Platform connects and manages applications, data, and devices via its API gateway. Wallarm seamlessly integrates with the MuleSoft gateway, bolstering app and API security.

Better Together

MuleSoft and Wallarm are powerful solutions that help enterprises achieve their business goals. MuleSoft helps organizations increase agility and innovation, reduce costs and complexity, and improve customer satisfaction. Leading organizations trust Wallarm for their API security needs, to reduce the risk of breaches and financial losses, improve compliance, and increase customer trust. Together, MuleSoft and Wallarm deliver all your API integration, management and security needs.

Benefits of Integrating Wallarm API Protection

By integrating Wallarm API protection with MuleSoft, organizations can unlock a host of benefits:



Comprehensive Enterprise API Protection

Wallarm provides comprehensive protection against a wide range of attacks, including OWASP Top-10 and emerging threats, API Abuse, Zero days, and more.



Seamless Policy Integration

Wallarm can easily be integrated with the MuleSoft API Gateway to create a unified platform for managing and securing API integrations.



Effortless Deployment

Wallarm's non-invasive reverse proxy deploys easily in front of MuleSoft.




Scalability via Automation

Wallarm offers automation and scalability to address the requirements of complex environments, minimizing the need for manual security.


How Wallarm Works

Wallarm sits in front of MuleSoft's API gateway and inspects all incoming API traffic. Wallarm uses a variety of techniques to identify and block attacks, including:




Signature-based detection

Wallarm maintains a database of attack signatures that it uses to identify known attacks.



Behavioral analysis

Wallarm analyzes the behavior of incoming API traffic to identify suspicious activity.

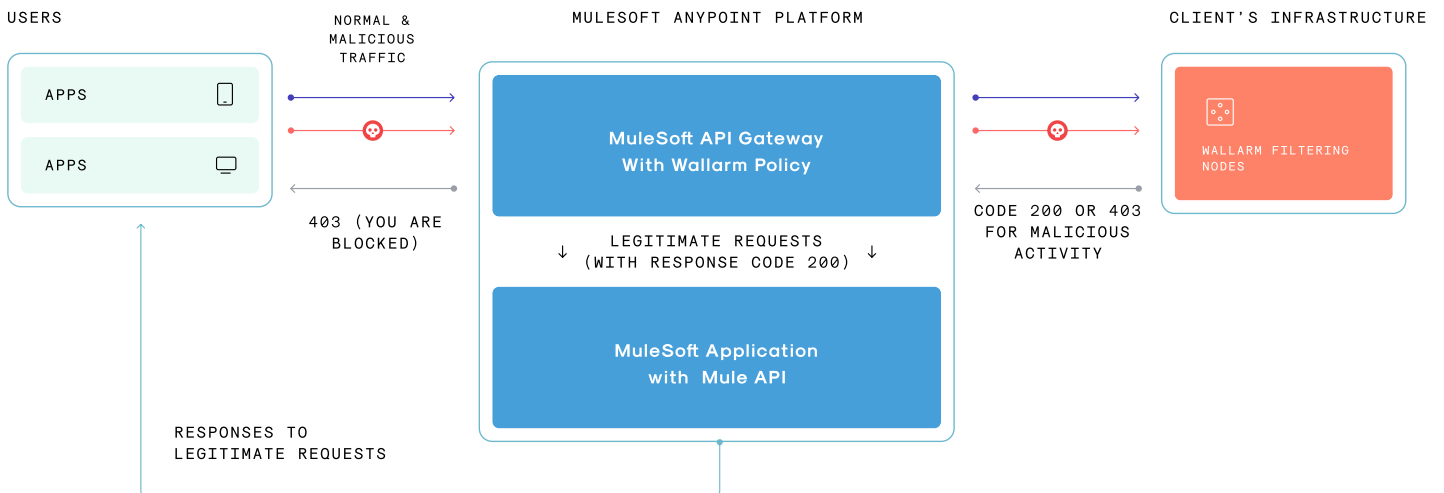


Machine learning

Wallarm uses machine learning to identify and block new and emerging attacks.

Wallarm / MuleSoft Solution Architecture

The following architecture diagram shows how Wallarm can be integrated with MuleSoft's API gateway. For organizations seeking comprehensive API security, Wallarm provides tailored MuleSoft integration compatible with a variety of deployment methods. It entails the external deployment of the Wallarm node and the application of security policies and custom code.



This configuration allows anonymized traffic to be routed to the external Wallarm node for analysis and protection against potential threats. Through this approach, Enterprises can ensure effortless integration, secure traffic analysis, risk mitigation, and the overall enhancement of their App and API security.