wallarm

PRODUCT DATASHEET

5 API Security Improvements for MuleSoft Deployments

A Maturity Model Approach

The development, deployment, and consumption of APIs is increasing exponentially. Organizations are building and using APIs to drive their businesses. At the same time, that increase in usage has driven a corresponding increase in API-based attacks and cybersecurity incidents. In order to address this increased threat, security teams must adopt a clear strategy for protecting their APIs, but how should you get started?

Wallarm has developed an API Security Maturity Model, based on the consolidated best practices from multiple sources, including vendors, community resources, and research. This maturity model approach points to 5 key improvements that organizations using MuleSoft should make to address API security.

DEVELOPER DRIVEN

First APIs

Get the Data Model Right

- **Secure Design:** Authentication, Authorization, Data Leakage, Encryption, Misconfiguration, 3rd party API Credential Management, Hardcoded Secrets
- **API Discovery:** Catalog Internal APIs

Growing Number of APIs

Secure Coding

- **Secure Design:** Centralized governance, Match Governance to risk, Incident Response
- **Bot Protection:** DoS Attacks
- **API Discovery:** Shadow APIs
- **Security Testing:** Regular Testing
- **Threat Protection:** Injection, SSRF, CSRF, XSS, MITM, Infrastructure, Reverse Engineering
- **Basic Rate Limiting**

SECURITY DRIVEN

Mature API Environment

Protect in Real-Time

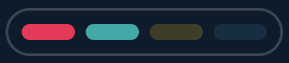
- **Secure Design:** Automate Governance Enforcement, Runtime Schema Validation
- **API Discovery:** Documentation (e.g. Documented Data Flows)
- **Security Testing:** API Specific Tooling
- **Threat Protection:** API Specific Tools, Behavioral protection, Real-time protection, ATO
- **Bot Protection:** Abuse Protection
- **Advance Rate Limiting**

High Security API Environment

Advanced Security

- **Security Testing:** Continuous Testing
- **Threat Protection:** Business Logic Flaws, Inspect Traffic Between Microservices

Implement API Discovery



You can't protect what you don't know about. API discovery is the foundational step for any API security program, enabling organizations to maintain an accurate inventory of all exposed endpoints. According to Gartner, 50% of APIs will go unmanaged by 2025, highlighting the critical need for comprehensive discovery.

MuleSoft provides API management features. Integrating Wallarm enhances this by automatically discovering and mapping out all active APIs within your infrastructure, including undocumented or shadow APIs that are often not managed with Mulesoft. This visibility allows teams to prioritize security efforts where it's needed most, particularly for APIs handling sensitive data that need to meet compliance requirements.

The benefit is clear: a comprehensive view of API traffic reduces the attack surface, making it harder for attackers to exploit unknown or unmonitored APIs. Moreover, API discovery ensures that developers have access to up-to-date API specifications, facilitating better collaboration and maintenance of API ecosystems.

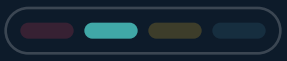
Implement Rate Limiting

Rate limiting is a fundamental feature of API management essential for developing secure APIs. This is particularly important because APIs are very easy to abuse for attackers, as they are fundamentally built to be consumed in an automated way. Such API abuse can result in attacks like credential stuffing, scraping, and DDoS attacks.

Rate limiting helps prevent abuse and overuse of APIs. MuleSoft allows organizations to set rate limiting rules at the API level using different strategies. Wallarm adds an extra layer by dynamically adjusting rate limits based on traffic patterns and potential threats. By integrating both, businesses can better control traffic and reduce the risk of attacks that exploit high volumes of requests.

Effective rate limiting mitigates resource exhaustion attacks, ensuring availability and performance are maintained even during unexpected surges in traffic. Even if there is a vulnerability in the API, strict rate limiting can help to slow down the attacker and gain time to mitigate the attack.

Centralize Authentication



A unified authentication framework is essential for ensuring secure access to APIs across various applications and services. MuleSoft supports a range of authentication methods, including OAuth2 and OpenID Connect, but combining this with Wallarm's security layer centralizes and strengthens identity verification.

Wallarm's security platform continuously monitors authentication workflows, detecting anomalies and preventing authentication bypasses or credential-stuffing attacks. Centralizing and securing authentication across all APIs ensures that unauthorized access is blocked, helping organizations safeguard sensitive data.

Detect and Block Attacks

APIs are an increasingly popular target for attackers, utilizing both simple attacks like SQL injection and complex attacks like API abuse. The OWASP API Security Top 10, a widely adopted framework for understanding API risks, highlights the growing sophistication of these threats. While traditional Web Application Firewalls (WAFs) or API Management solutions may offer some protection, they often fall short when dealing with more advanced API-specific vulnerabilities.

Wallarm's advanced AI-driven threat detection and blocking capabilities allow for real-time mitigation of malicious behavior. Through a unique deep API call inspection capability, Wallarm thoroughly examines more API protocols and a greater portion of each request to identify obfuscated attacks. This level of scrutiny enables the detection of sophisticated API threats that may bypass conventional security measures. Integration with MuleSoft API gateways allows for easy capture of traffic and real-time blocking actions in MuleSoft environments.

Wallarm can detect suspicious requests based on both known vulnerabilities and emerging threats, automatically blocking attacks without human intervention. This continuous monitoring and response helps organizations defend against API threats before they can be exploited.

Implement API Governance

API governance is critical for consistency, security, and compliance across API deployments. MuleSoft's API management features help enforce policies, standards, and best practices. Integrating Wallarm's security controls automates enforcement of API specifications and granular security policies. This ensures compliance with requirements like GDPR or HIPAA, while monitoring API security posture over time.

API discovery features aid in identifying APIs to enforce compliance. Wallarm's dashboard demonstrates how existing security controls ensure compliance according to the NIST CFP framework. Implementing strong governance with real-time security insights reduces the risk of misconfigurations or insecure APIs in production.