wallarm

PRODUCT DATASHEET

Threat Replay Testing

Turn attackers into your own penetration testers

The need for API security testing

The digital transformation in enterprises has led to the meteoric rise in the use of APIs. APIs are the key enablers of this digital revolution connecting users, with data and infrastructure. As of 2023, there are over 1.3B active APIs [*] . This makes APIs as one of the most prolific attack vectors being exploited by bad actors. Cybersecurity teams rely on API security testing to identify vulnerabilities and safeguard APIs. Traditional security testing measures can be limited in scope and may not uncover all potential weaknesses. Bad actors often probe systems in ways that traditional security methods might not anticipate, leaving some vulnerabilities undiscovered. On top of this, companies are looking for real-time testing, which constantly requires additional tuning, which is both time-consuming and requires proper expertise and tooling. This is where API security testing becomes essential to ensure the integrity and security of sensitive data and resources.

The Traditional API security Testing Approach

API security testing involved methodically assessing the enterprises' entire API inventory for potential vulnerabilities against unauthorized access, data breaches, injection attacks, and other security risks. In order to conduct API security testing, security teams need to develop a comprehensive checklist encompassing key aspects of testing that includes setting up the right test environment, defining the scope of the testing, and using the appropriate tools for testing. Security teams configure security tools which require domain expertise to generate real-time security testing, which is often based on synthetic inputs through automated tools or scripts designed to simulate various attack vectors like SQL injection, cross-site scripting (XSS), or other types of vulnerabilities. Tools like OWASP ZAP, Burp Suite, or custom scripts are used to create these synthetic requests to test how an application would react to malicious or unexpected inputs.

Traditional dynamic application security testing (DAST) scanners cannot cover APIs completely; they cover only a small portion of them. If an organization's front end does not interact with all API endpoints, traditional DAST scanners will miss them. It is therefore essential to adopt a modern, dynamic API security testing strategy that targets issues in all an API's endpoints.

Modern API Security Testing Approach with Wallarm

Threat Replay Testing identifies vulnerabilities by replaying real-world attack. This proactive approach addresses the limitations of traditional security testing, which is often based on synthetically created inputs. By continuously monitoring and analyzing attack traffic, organizations can stay ahead of emerging threats and test their applications and APIs in real time. Security teams are able to get automatically generated real-time security tests based on real-world incoming attacks on their systems. This approach allows the security teams to assess how real-world attackers approach their production environments for vulnerabilities. TRT does not replace the DAST tools but is an additional tool in the arsenal of the security teams.

BOOK A DEMO

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

wallarm

PRODUCT DATASHEET

Key Benefits of Threat Replay Testing

Real-time analysis

It uses actual attack data to identify vulnerabilities that are being actively exploited or have the potential to be exploited in the future.

Comprehensive testing

By generating variations of real attacks, it explores different attack vectors and exposes weaknesses the original attackers may have missed.

Safe simulation

It removes harmful code and sensitive authentication details from the test requests, ensuring that the testing process doesn't cause any damage or compromise systems.

Non-production testing

It allows testing applications and APIs in a safe environment (typically staging) without risking production data or system stability.

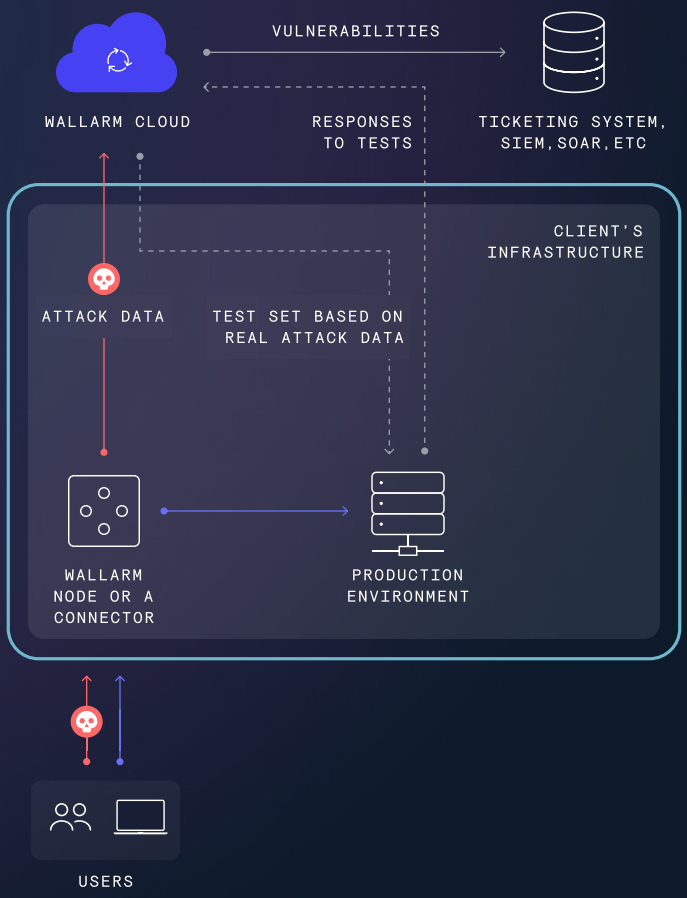
CI/CD Integration

It can be implemented as a part of the development cycle by sending test requests to the API services in a pre-production environment.

How does Threat Replay Testing work?

TRT turns attackers into your own penetration testers. It analyzes initial attack attempts and then explores other ways to exploit the same attack. This helps organizations cover the entire attack surface.

You simply set up test policies to convert attacks into security tests.Then define your staging environment, select target endpoints and attack types. Wallarm automatically sanitizes replayed payloads to prevent data corruption or crashes and allows TRT to be even more secure by acting on staging environments.



BOOK A DEMO

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