wallarm

It's Not API Security

If it Doesn't Block Attacks

Navigate through our detailed comparison of API Security products, designed to help you identify the right fit for your specific needs. Gain clarity and insight to choose the most suitable API security solution confidently.

wallarm

SALT

Akamai

TRACEABLE

CLOUDFLARE

Overview

Security teams are tasked with the challenge of securing the ever expanding API attack surface while maintaining application performance. Application security decision makers need to follow a structured approach aligned with security and business objectives when evaluating API security tools. In this document we will enumerate the critical assessment criteria that can help your organization make the right choice for securing your APIs.

The assessment criteria should align with the four stages in the API security lifecycle which are: discover, protect, respond, and test. In the first step, teams need the right tools, starting with complete visibility into the entire API landscape including identifying all APIs, both internal and external. The second step after discovery is to protect your discovered APIs against attacks, including traditional attacks and more complex business logic abuse. The third step involves automating the remediation and mitigation process to help security teams respond faster to existing and new API threats. The final step involves automating testing for APIs and applications so that the security teams are able to detect potential vulnerabilities and mitigate those earlier in the development cycle, minimizing their impact in production environments.

Finally, the evaluation criteria for the right API security tool also needs to include coverage for any new emerging technologies or frameworks that might expose organizations to new threats. For example, generative AI and agentic AI have upended the enterprise world with new opportunities for development teams, but at the same time they have also created new challenges for security teams. Similarly, as enterprise infrastructure is evolving, security teams are challenged by the deployment and management of effective security consistently across this new hybrid infrastructure in a way that minimizes the impact to users and applications. In the next section we will cover each of these criteria, their importance to security teams, and how Wallarm is uniquely positioned to solve the challenges over competition.

API Discovery & Posture Management Discover

Wallarm differentiates itself from other API security solutions by offering a comprehensive platform to safeguard your complete API portfolio. This integrated approach means there's no need to invest in additional third-party products, streamlining your security measures and providing comprehensive protection in one single unified solution.

WHY WALLARM

While most API security tools provide basic discovery of API endpoints, Wallarm is differentiated by its privacy first approach, avoiding creating a third party data lake of sensitive API data, by its ability to automatically identify sensitive business flows, including AI APIs. Wallarm also offers the ability to actively enforce API specifications.

	WALLARM	SALT	AKAMAI	TRACEABLE	CLOUDFLARE
Automatically discover internal and external APIs	✓	✓	✓	✓	✓
Data analyzed on customer premises (privacy-first approach)	✓	–	–	–	–
AI Endpoint Discovery	✓	–	–	–	–
Primary posture	✓	–	–	–	–
OpenAPI Specification Enforcement	✓	–	!	–	✓

Real-time detection and protection Protect

Security teams need more than just API threat detection. Attackers can steal data from APIs in under a minute, making real-time blocking imperative. Traditional API security tools lack the enforcement capabilities to block attacks, leaving the security teams struggling to secure their APIs.

WHY WALLARM

Wallarm is unique in its support for inline deployment, including near-zero latency, through its cloud-native connectors. Unlike other API security vendors, which only offer detection and depend on third-party solutions like WAFs or API Gateways for limited mitigation, Wallarm blocks attacks in real-time to protect your APIs.

	WALLARM	SALT	AKAMAI	TRACEABLE	CLOUDFLARE
Real-time blocking	✓	–	⚠	✓	⚠
Blocking API Sessions	✓	–	–	–	–
Credential Stuffing Detection	✓	–	–	–	–
Zero-Day Vulnerability Protection	✓	–	–	–	–
Account Takeover	✓	–	–	–	–

API Attack Surface Management Respond

Attackers are constantly probing your organization's API attack surface for entry points and weaknesses. It's important that security teams stay ahead of attackers by identifying risks before they can be exploited, but attack surface management tools don't understand APIs and API security tools don't provide an external API attack surface perspective.

WHY WALLARM

Wallarm provides an innovative solution to gain comprehensive control over your expanding API ecosystem. API Attack Surface Management (AASM) is an agentless detection solution, designed to discover external hosts with their APIs, identify missing security controls, discover vulnerabilities, and mitigate API Leaks. Additionally Wallarm provides the capability to search for and catalog any leaked secrets, thereby minimizing the time to secure the attack surface, resulting in a better security posture.

	WALLARM	SALT	AKAMAI	TRACEABLE	CLOUDFLARE
API Attack Surface Discovery	✓	✓	–	✓	–
Security Controls Testing	✓	✓	–	✓	–
API Gateway Detection	✓	–	–	–	–
API Leak Management	✓	–	–	–	–

Minimize risks through API security testing Test

As organizations “shift left” to incorporate security into the development process, they are testing APIs earlier to discover any potential vulnerabilities. Traditional appsec testing tools perform poorly against APIs, leaving opportunities for attackers to exploit. Test scenarios are typically built using traditional synthetic inputs which leaves room for real-world exploits.

WHY WALLARM

Wallarm uses a unique and innovative approach to testing APIs that involves both traditional testing methods and new capabilities like Threat Replay Testing. By discovering vulnerabilities before they go live in production, Wallarm allows teams to reduce risk and fix issues early as a part of their DevOps process. These features help security teams to identify vulnerabilities, test the resilience of the system against unexpected or malformed input, and simulate real-world attacks to assess the security of the API.

	WALLARM	SALT	AKAMAI	TRACEABLE	CLOUDFLARE
Threat Replay Testing	✓	–	–	✓	–
Active API Vulnerability Scanning	✓	✓	✓	✓	–
Passive API Vulnerability Detection	✓	–	–	–	–
AI Penetration Testing	✓	–	–	–	–
Schema-Based Testing	✓	✓	✓	✓	–

Protect Agentic AI and Gen AI applications Emerging Technology

As enterprises embrace agentic AI for transformative business opportunities, they face a critical challenge: ensuring these intelligent systems operate securely. APIs serve as the connective tissue between AI models and applications; they're also now the primary attack vector for AI-driven environments. Traditional security solutions lack the depth to protect against this new attack vector.

WHY WALLARM

Wallarm is the only API security solution that delivers AI-native security for AI agents and multi-agent systems. It protects your AI applications against injection attacks, data leakage, and unauthorized access while protecting enterprise-critical systems.

	WALLARM	SALT	AKAMAI	TRACEABLE	CLOUDFLARE
Prompt Filtering	✓	✓	⚠ Separate Product	✓	—
Response Validation	✓	—	—	✓	—
Real-time blocking	✓	—	✓	—	—
Custom Protection Policies	✓	✓	⚠ Separate Product	—	—
Penetration Testing for Agentic AI	✓	—	—	—	—

Deployment Flexibility

As enterprise networks are evolving, how they build and leverage APIs is also evolving. Most organizations are moving towards a hybrid infrastructure, typically involving a combination of public and private cloud, as well as on-premises data centers. Hybrid organizations have to secure APIs across their distributed and cloud infrastructure.

WHY WALLARM

Wallarm supports a wide variety of customer architectures with the most flexible deployment available, both out-of-band (ePBF) and inline with near-zero latency. Built from the ground up to protect both legacy and cloud-native tech stack, Wallarm provides the coverage across an organizations entire hybrid infrastructure.

	WALLARM	SALT	AKAMAI	TRACEABLE	CLOUDFLARE
In-line/agent-based	✓	–	!	–	!
Out-of-band/agentless	✓	✓	!	✓	–
Security Edge (CDN or Cloud hosted)	✓	–	!	–	✓
Private/Legacy Infrastructure	✓	–	–	–	–
Managed API Security	✓	–	✓	–	–