AI-POWERED SECURITY

Protect Applications and APIs in the Cloud

The Wallarm platform includes real-time protection (NG-WAF), threat verification (DAST), and AI behavioral analytics working together in a comprehensive application security build for the modern technology stack.

Real-time Application Protection

- Cost-effective protection for application and APIs against full spectrum of threats: OWASP Top 10, bots, app abuse and DDoS
- Works in full blocking mode (ultra-low false positives) to satisfy compliance requirements
- Dynamic application-specific security rules created automatically
- Centrally managed distributed architecture
- Cloud-native and integrated with DevOps stack

Security Testing

- Active threat verification for discovering application-specific vulnerabilities
- Active and passive vulnerability testing
- Discovery of publicly exposed assets, network services, and ports
- Great for DevOps team with CI/CD

Wallarm offers an adaptive security platform including an integrated web vulnerability scanner and Next Generation WAF solution with automatically generated security rules based on AI.

Chris Rodrigues
FROST & SULLIVAN
Security is a priority for MedNet Solutions. As a part of migrating MedNet Solutions’ EDC product, iMedNet, to AWS, implementing reliable, scalable security was of paramount importance. MedNet Solutions needed to implement Web Application Firewall (WAF) security at the request of customers and to meet HIPAA compliance requirements.

### APPLICATION PROTECTION ALTERNATIVES

<table>
<thead>
<tr>
<th></th>
<th>Open source WAF</th>
<th>CloudFlare &amp; other CDN add-ons</th>
<th>Legacy hardware WAF</th>
<th>Wallarm NG WAF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection against web treats (OWASP Top 10 etc.), bots, and other threats</td>
<td>Requires manual tuning</td>
<td>Basic signature-based protection</td>
<td>Requires manual tuning</td>
<td>Yes</td>
</tr>
<tr>
<td>Smart API protection</td>
<td>No</td>
<td>No</td>
<td>Limited</td>
<td>Yes, REST/XML/JSON including nested formats</td>
</tr>
<tr>
<td>TCO/Required IT hours</td>
<td>80+ hours per month</td>
<td>40+ hours per month</td>
<td>60+ hours per month</td>
<td>~ 5 hours per month</td>
</tr>
<tr>
<td>False Positives</td>
<td>Too high for blocking</td>
<td>Too high for blocking</td>
<td>Too high for blocking</td>
<td>Near zero false-positives with no manual tuning</td>
</tr>
<tr>
<td>Cloud Native development / DevOps oriented</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Wallarm Nodes**

Inspect traffic & block malicious requests.
ACTIVE THREAT VERIFICATION
AI-POWERED TESTING

Scanner checks every payload
Sending out a series of requests against the application to see if it’s vulnerable to attack.

Extracts payloads from attacks
Wallarm extracts a payload, combines it with the information about which part of the application it was targeting & creates a job for the cloud-based scanner.

Reporting an incident
A ready-to-use ticket is created for security issues & the team is notified.

Updates Security
Custom security rules are deployed to Wallarm Nodes.

DAST ALTERNATIVES
Wallarm active threat verification provides improved visibility and provides actionable intelligence. It helps assess the risk of detected security events, which in turn reduces signal-to-noise ratio. A unique feature of Wallarm, Active Threat Verification is a part of the Wallarm DAST module that also includes asset discovery and testing for known vulnerabilities, which also takes into account the application logic detected by the NG-WAF component—all without the browser crawling!

<table>
<thead>
<tr>
<th></th>
<th>Quals</th>
<th>Nexus</th>
<th>Wallarm Scanner</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asset discovery</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>App DAST</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Regression Tests</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Attack re-checker</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Web-management interface provides a near real-time view of the traffic along with information about attack and incidents.
Advantages of Wallarm AI

As applications and attacks grow in complexity and sophistication, traditional protection methods become more cumbersome or break altogether.

Wallarm’s approach is principally different from legacy approaches that rely on signatures and have a lot of false positives. This approach relies on AI to profile applications and to decide what’s normal within the application profile.

The combination of on-site analysis of application requests and responses with cloud-driven reinforcement learning is what allows Wallarm to be

- Fast
- Accurate
- Comprehensive
- Auto-configurable

Automated application environment learning makes Wallarm a good fit for highly distributed infrastructures that change often. It also means that it can detect zero-day threats, in addition to threats that are known, and eliminate many false positives and false negatives by generating a smaller number of security rules that are specifically relevant to the applications under protection.

About Wallarm

Wallarm is an innovative AI startup focused on the security of websites, microservices, and APIs running on public and private clouds.

We have some unusual features in our web, so we needed a company that could adapt their product to us. With Wallarm AI, we successfully identify and block attacks on our product, without dedicated effort from our security team and getting excellent protection

SEMrush security team
www.semrush.com