The Future of Application Security: WAAP

Comprehensive Protection for Web Applications and APIs in a Threat-Driven World

15 Highlights from our Buyer's Guide

www.imperva.com

imperva
a Thales company

Introduction to WAAP

WAAP is a comprehensive solution that protects web applications and APIs from modern security threats, including those outlined by the OWASP Top 10.

WAAP became an industry term in 2017 to address the evolving complexities of application security, ensuring protection against a broad range of runtime attacks.

The Importance of Application Security

As applications drive global influence and serve as primary business models, securing them from threats is essential.

More than 85% of organizations experienced a successful cyberattack in 2021, highlighting the critical need for robust application security.

Evolving Threat Landscape

As security threats become more sophisticated and increase in volume, traditional security measures are no longer sufficient.

Between January and December of 2021, Imperva recorded a 148% increase in account takeover attacks, demonstrating the escalation of threats.

The Evolution from WAF to WAAP

Traditional Web Application Firewalls (WAFs) are no longer enough; WAAP provides a more robust and comprehensive security solution.

WAAP includes next-generation WAF, API security, bot protection, and DDoS protection, offering a holistic defense against sophisticated threats.

Importance of Comprehensive Security

Simply meeting compliance requirements is not enough; organizations must ensure their applications are fully protected to prevent breaches.

Many organizations mistakenly believe that meeting OWASP Top 10 compliance guarantees security, but true protection requires a more comprehensive approach.

Imperva’s WAAP Solution

Imperva’s WAAP solution offers enterprise-class protection against the most sophisticated security threats, tailored for cloud, on-premises, or hybrid environments.

Imperva’s WAAP integrates multiple security technologies, ensuring high-performance protection against emerging threats like SQL injection, cross-site scripting, and illegal resource access.

API Security: A Critical Component

With the rise of microservices and APIs, visibility and protection of API endpoints are more important than ever.

Imperva API Security provides automatic detection and classification of APIs, enabling comprehensive visibility and risk assessment without disrupting development workflows.

DDoS Protection

DDoS attacks can cripple business operations, but Imperva's WAAP solution provides powerful, low-latency protection.

Imperva provides near-zero latency Network DDoS protection, backed by a 3-second SLA for Always-On mode, ensuring that legitimate traffic is not disrupted.

The Rise of Ransomware and RDoS

Ransomware and Ransom Denial of Service (RDoS) attacks are on the rise, targeting high-profile sectors like financial services and retail.

Ransomware attacks increased from every 40 seconds in 2016 to every 11 seconds in 2021, necessitating robust protection measures.

Combating Sophisticated Bot Attacks

Bots are becoming increasingly sophisticated, making traditional detection methods ineffective.

Imperva’s Advanced Bot Protection uses a multilayered detection process with machine learning to accurately differentiate between human, good bot, and bad bot traffic.

The Challenge of Alert Fatigue

Imperva’s WAAP solution combats alert fatigue by distilling millions of security events into prioritized security insights.

Attack Analytics integrates all WAAP tools into a central location, offering contextual reporting and actionable recommendations to enhance security posture.

Improving Performance with CDN

Imperva’s Content Delivery Network (CDN) improves website content delivery, ensuring fast and reliable access across the globe.

Imperva’s global network of PoPs reduces page load times and optimizes content delivery, enhancing user experience and reducing bandwidth costs.

WAAP: More Than the Sum of Its Parts

WAAP is not just about advanced functionality, it's also about building a cybersecurity partnership with customers.

Imperva's SaaS model includes threat research, machine learning, and ease-of-use reporting out-of-the-box, unlike other vendors that require expensive add-ons.

The Role of Customer Support in WAAP

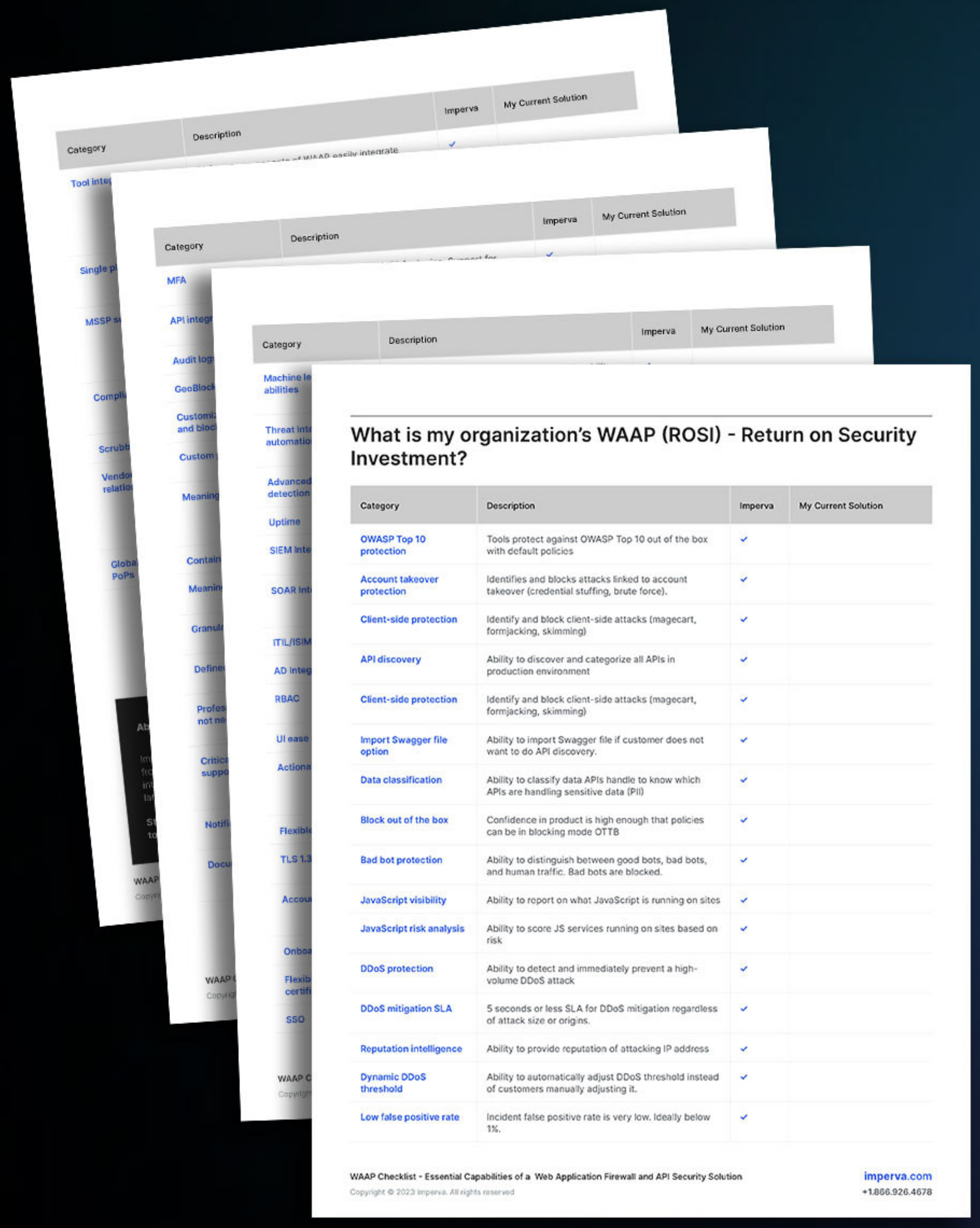
Effective WAAP solutions include robust customer support and professional services to ensure successful implementation and use.

Imperva's WAAP solution is enterprise-ready, providing integrated platform services out-of-the-box to meet diverse business needs.

Conclusion

Imperva's WAAP solution is a proven, complete security stack that protects SMBs and enterprises from today's most sophisticated threats.

With a growing number of points of presence (PoPs) worldwide, Imperva's WAAP tools, including Cloud WAF, Advanced Bot Protection, and API Security, are just a click away.



What is my organization's WAAP (ROSI) - Return on Security Investment?

Category	Description	Imperva	My Current Solution
OWASP Top 10 protection	Tools protect against OWASP Top 10 out of the box with default policies	✓	
Account takeover protection	Identifies and blocks attacks linked to account takeover (credential stuffing, brute force).	✓	
Client-side protection	Identify and block client-side attacks (magecart, formjacking, skimming)	✓	
API discovery	Ability to discover and categorize all APIs in production environment	✓	
Client-side protection	Identify and block client-side attacks (magecart, formjacking, skimming)	✓	
Import Swagger file option	Ability to import Swagger file if customer does not want to do API discovery.	✓	
Data classification	Ability to classify data APIs handle to know which APIs are handling sensitive data (PII)	✓	
Block out of the box	Confidence in product is high enough that policies can be in blocking mode OTTB	✓	
Bad bot protection	Ability to distinguish between good bots, bad bots, and human traffic. Bad bots are blocked.	✓	
JavaScript visibility	Ability to report on what JavaScript is running on sites	✓	
JavaScript risk analysis	Ability to score JS services running on sites based on risk	✓	
DDoS protection	Ability to detect and immediately prevent a high-volume DDoS attack	✓	
DDoS mitigation SLA	5 seconds or less SLA for DDoS mitigation regardless of attack size or origins.	✓	
Reputation intelligence	Ability to provide reputation of attacking IP address	✓	
Dynamic DDoS threshold	Ability to automatically adjust DDoS threshold instead of customers manually adjusting it.	✓	
Low false positive rate	Incident false positive rate is very low. Ideally below 1%.	✓	

WAAP Checklist - Essential Capabilities of a Web Application Firewall and API Security Solution

imperva.com
+1.866.926.4678

Essential Capabilities of a WAAP Checklist Checklist

- OWASP Top 10 protection
- Account takeover protection
- Client-side protection
- API discovery
- Import Swagger file option
- Container protection
- Block out-of-the-box
- Low false positive rate
- Plus 50 more important criteria to evaluate

Get the WAAP checklist here:

https://utm.io/uhlzm

About Imperva Application Security

Imperva protects customers from cyber attacks through all stages of their digital transformation.

- Cloud and On-Prem Web Application Firewall (WAF) solutions
- API Security for continuous protection of all APIs
- Advanced Bot Protection for websites, mobile apps, and APIs
- Client-Side Protection for websites & PCI DSS 4.0 compliance
- DDoS protection for websites, networks, and DNS
- Runtime Application Self-Protection (RASP) for security by default
- Content Delivery Network (CDN) for secure content & app delivery

Learn more at **www.imperva.com**

imperva
a Thales company