White Paper

Imperva

WAAP Buyers Guide

Essential Capabilities of a Web Application Firewall and API Security Solution

thalestct.com

THALES
Building a future we can all trust

THALES

Application Security today

Applications have become mission-critical for organizations looking to drive rapid growth. They help facilitate an organization's influence around the world and can act as the primary business model. These applications require protection from security threats, yet end-users demand high availability and an uninterrupted experience, which can make for a tough balancing act. On top of that, security threats are becoming more sophisticated and growing in volume. **"More than six out of seven organizations (85.3%) experienced a successful cyberattack in 2021."**

Most organizations say they see security as a must, but, internally, many see security as a box that to be checked to meet requirements and regulations. This means budgets for security have been stagnant in recent years, while the need to implement security controls is growing as attacks become more prevalent and complex. Between January and December of 2021, Imperva noted a staggering 148% increase in account takeover attacks. Security teams are expected to keep up with development teams' innovation while also not hindering growth through vulnerability mitigations. Security vendors must adjust to how the industry approaches security. Solutions need to enable rapid application development while keeping applications safe from the latest attacks. In the ever-evolving threat landscape, the legacy web application firewall (WAF) is no longer enough; vendors need to provide robust solutions that protect applications and their APIs from both bad actors and bad bots. Web Application and API Protection (WAAP) is the new way for organizations to implement application security.

WAAP is the natural evolution of web application protection.

What is WAAP

Gartner coined the term WAAP. It's defined as "cloud web application and API protection platforms mitigate a broad range of runtime attacks, notably the Open Web Application Security Project (OWASP) top 10 for web application threats, automated threats and specialized attacks on APIs." As applications become more complex and evolve, so do their security needs. OWASP recently updated the list of top 10 web application security risks; most legacy WAFs do not protect against this new list of attacks. WAAP is a suite of tools that includes next-generation WAF, API security, bot protection, and DDoS protection. Combined, these tools are a powerful force against sophisticated threats and attacks.

Why Does WAAP Matter

Web applications are the front door to most environments and, thus, a way to access customer data. Many organizations view applications as inherently secure because they have tools in place to mitigate the vulnerabilities mentioned in the OWASP Top 10. This approach to security isn't atrocious but isn't ideal either. Simply checking a box to meet security compliance requirements is not application protection, it can lead to potential breaches.

Prioritizing meeting compliance requirements over ensuring that applications are adequately protected has been a known issue in the cybersecurity space for years. Security teams have been tasked with securing as much as possible without slowing the organization down.

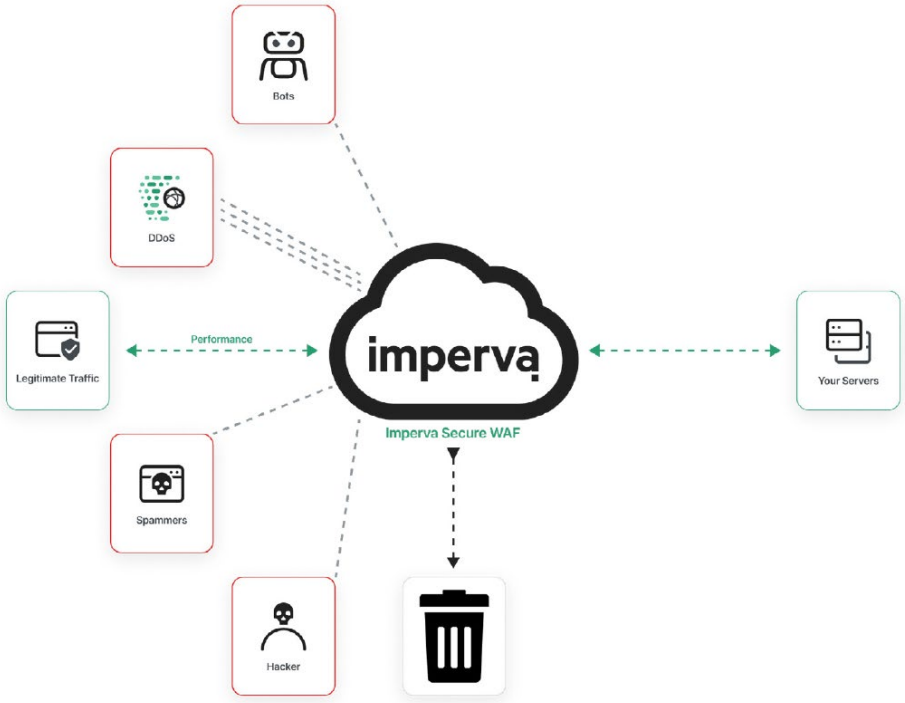
Additionally, vendors have presented organizations with traditional, outdated approaches to new, complex security threats. These traditional rules and signature-based tools will never be able to truly keep up with today's development teams or emerging security threats. With more open-source application code and API adoption growing, security is always going to be an afterthought. Developers are not always interested in fixing their insecure code, they are instead focused on the speed of growth for the organization. WAAP is the response to these issues: this suite of solutions holistically protects and gives visibility to all web-facing applications and APIs.

The WAAP Recipe (DDoS, CSP, BOT, ATO, API Security, ML & Analytics)

Imperva WAAP offers the industry's leading web application security, providing enterprise-class protection against the most sophisticated security threats. Whether your websites and applications are hosted in the public cloud, on-premises, or hybrid environment, Imperva's WAAP solution ensures that your critical assets are always protected against any type of application layer attack.

"By 2024, 70% of organizations implementing multicloud strategies for web applications inproduction environments will favor cloud web application and API protection platform(WAAP) services over WAAP appliances and IaaS-native WAAP."

Gartner

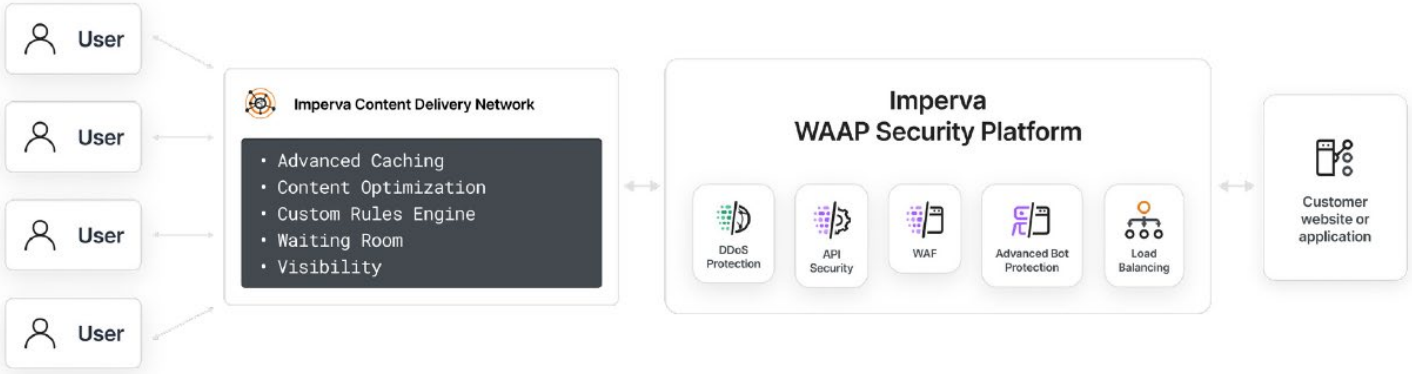


How Imperva Cloud WAF Works

Imperva deploys an integrated and comprehensive application security model. This approach provides a defense-in-depth approach to enforcing security from the application to the end user. A leader in the Gartner Magic Quadrant for **Web Application Firewalls and API security (WAAP)**, Imperva provides WAF solutions (cloud-based Cloud WAF and on-premises or virtual appliance WAF Gateway) to defend against all known OWASP Top 10 and emerging threats, including SQL injection, cross-site scripting, and illegal resource access.

As developers build and integrate microservices and APIs across enterprise applications, the need for visibility into these API endpoints is greater than ever. Whether it's a known edge API, an unknown shadow API, or internal API driving transactions on the backend, discovering and classifying APIs is essential for establishing a positive security model for API Security. Through automatic detection of API endpoints, Imperva **API Security** enables comprehensive API visibility for security teams by providing contextual data and tags; this tool also automatically determines risks around sensitive data. API Security can be easily injected into an organization's SDLC as it does not require developers to publish APIs via OpenAPI or by adding resource-intensive workflows to their CI/CD processes.

Cybercriminals often wage disruption campaigns against high-profile targets. Organizations, especially those in the previously listed sectors, are at risk of **Distributed Denial of Service (DDoS)** attacks. Without proper protection against malicious bots and DDoS attacks, organizations are at risk of poor user experience due to slowed or denied access to their websites. Constant attack campaigns can drive away users, fulfilling the goal of the attacker. Ransome Denial of Service (RDoS) and Ransomware have been on the rise. According to a report by Cybersecurity Ventures, ransomware attacks increased from every 40 seconds in 2016 to every 11 seconds in 2021. Threat actors like REvil (a ransomware-as-a-service organization) are making a resurgence in activity in 2022. A comprehensive WAAP solution should provide powerful DDoS protection that eliminates attacks long before malicious traffic reaches a customer's website. Imperva offers near-zero latency and backed by a 3-second service level agreement, DDoS traffic is mitigated without disruption to legitimate traffic.



Organizations that depend upon return users often require robust infrastructure that is able to support the quick delivery of web content to meet global user demand. **Content Delivery Networks (CDN)** the backbone of Imperva Application Performance, improves website content delivery and keeps costs down with intelligent caching, load balancing and automated failover to efficiently deliver web applications around the globe. With a global network of PoPs, Imperva is able to provide quick and reliable access to web content. Imperva helps deliver faster page load times and reduce bandwidth with advanced caching, content optimization and load balancing for improved site performance and a superior user experience.

While bots have been wreaking havoc on the internet for years now, their level of sophistication continuously increases, as they become much harder for traditional tools to detect and mitigate. They evade detection by cycling through random IPs, entering through anonymous proxies, changing their identities, mimicking human behavior, delaying requests, and more. **Advanced Bot Protection** safeguards websites, mobile apps and APIs from these advanced automated threats that abuse business logic. It does so by utilizing a multilayered detection process which includes reputational analysis, an advanced client classification engine, and proprietary machine learning algorithms developed by Imperva to determine whether traffic is coming from a human, a good bot or a bad bot.

Most importantly, It does so swiftly, with pinpoint accuracy and without affecting legitimate, critical traffic. The generic bot protection offered by many WAF vendors isn't advanced enough to provide adequate protection against these automated threats. Many legacy WAF offerings aren't able to detect and deter these types of attacks by highly sophisticated bots in real time, or they only provide some visibility without actions, leading to this malicious traffic getting through.

"By 2026, more than 40% of organizations with consumer-facing applications that initiallyrelied only on a WAAP for bot mitigation will seek additional anomaly detectiontechnology from specialized providers"

Gartner

With the complex and ever-changing threat landscape, it's more important than ever to have visibility across your data and applications. An overwhelming amount of security alerts can keep security teams from discovering critical attacks that pose an imminent threat. **Attack Analytics,** a key part of Imperva's WAAP solution, combats alert fatigue by distilling millions of security events into a prioritized set of security insights. Put another way, all the WAAP tools are integrated into a central location to provide ease of reporting and context behind individual alerts. It also gives recommended actions to improve your security posture, helping you recognize your cyber risk and decrease it.

TCO : WAAP Is More Than A Sum Of Its Parts

As discussed above, WAAP is the next evolution of application security. It is more than just advanced functionality and "next-gen cyber security"; it is a partnership between the customer and the vendor. Consumers have rightfully demanded more from security vendors for years and the industry has been struggling to meet demands. There have been some unspoken cracks during this rush to innovate, the expectations between vendors, and the Infosec teams using their products. Many vendors are aware of these issues and tend to try to fix the issue by adjusting or developing a one-off tool to only mitigate the crack. This approach does not answer for the overall issue of not creating a truly integrated application security suite with multiple functionalities and support infrastructure to help implement it into different environments.

When looking at the many WAAP options available ask do they have an integrated platform with enterprise-ready services out-of-the-box.

Vendor	OWASP	Bot	Layer 7 DoS	Resiliency	Vul. Web Environment	Complete Security Score
Akamai	86%	17%	40%	63%	80%	60%
Cloudflare	84%	17%	80%	55%	70%	63%
F5	93%	67%	100%	69%	100%	84%
Imperva	95%	100%	100%	68%	75%	91%
Average	88%	50%	81%	63%	75%	73%

Customer support and professional services are cornerstones of the WAAP approach. Customers should not be expected to know how to set up and use new tooling out of the box. The above chart shows the out-of-the-box functionality of the 4 leaders in the WAAP space. As the chart shows, many vendors require expensive add-ons to make their WAAP solution complete. Imperva's SaaS model makes most of this a moot point, with threat research, machine learning, attack analytics, and ease of use reporting.

The Takeaway

Organizations today need a security solution that will work for the future applications to come, not just secure their legacy software and applications. With the rapid adoption of new technologies in application development, application modernization has become the norm while securing that journey has continued to be difficult. Budgets will always be tight, development will always be quick and agile, and attackers know this. Having an out-of-the-box solution that protects your whole web application pipeline while continuing to make advancements to protect from the unknown seems like a dream. Imperva has been doing just that for 20 years.

Imperva Application Security stack is a complete solution that has a proven track record for any size enterprise. Helping companies large and small stay protected with our WAAP solution containing industry-leading integrated security.

Imperva solutions are available for sale to the U.S. Federal Government through Thales Trusted Cyber Technologies.

About Thales Trusted Cyber Technologies

Thales Trusted Cyber Technologies, a business area of Thales Defense & Security, Inc., is a trusted, U.S. provider of cybersecurity solutions dedicated to U.S. Government. We protect the government's most vital data from the core to the cloud to the edge with a unified approach to data protection. Our solutions reduce the risks associated with the most critical attack vectors and address the government's most stringent encryption, key management, and access control requirements.

For more information, visit www.thalestct.com

Contact us - For office location and contact information, please visit thalestct.com/contact-us

©2024 Thales 3.29.24