2025

# The history of the Web Application Firewall (WAF) and how Webouncer will replace it

WAF VS. WEBOUNCER (EP4430501)

CARSTEN KLEIN

KRALOS GMBH | Burgdorf - Germany

# Index

# The development of the Web Application Firewall (WAF)

The history of the Web Application Firewall (WAF) begins in the late 1990s, when the Internet was gaining in importance and web applications were increasingly becoming the target of cyber-attacks. At that time, traditional network firewalls, which operate on layers 3 and 4 of the OSI model, were not sufficient to defend against the more complex threats on the application layer (layer 7). Attacks such as SQL injection or cross-site scripting (XSS) required a specialized security solution.

## Early years (1990s to early 2000s):

The first WAFs were created as rudimentary filters for HTTP traffic. They were often simple rule-based systems that blocked known attack patterns ("blacklisting"). Companies such as Imperva and F5 began to develop products specifically aimed at protecting web applications. These early WAFs were mostly hardware-based and deployed on-premises.

## Mid-2000s- OWASP and standardization:

WAF development received a boost with the founding of the Open Web Application Security Project (OWASP) in 2001 and the publication of the OWASP Top 10 (first published in 2003). WAFs were designed to specifically combat the most common vulnerabilities such as SQL injection or XSS. "Whitelisting" approaches also emerged, in which only known, secure traffic was permitted.

## 2010s- Cloud and AI:

With the advent of the cloud computing era (e.g. Amazon Web Services, launched in 2006), WAFs became more flexible. Cloud-based WAFs such as those from Cloudflare or Akamai offered scalability and simplicity over traditional appliance solutions. At the same time, more advanced WAFs integrated machine learning to dynamically respond to new threats instead of just using static rules.

## Modern WAFs (2020s):

Today, WAFs are often part of comprehensive security platforms (e.g. WAAP - Web Application and API Protection) that combine DDoS protection, bot management and API security. Nevertheless, they remain reactive: they are based on known signatures or anomaly detection and often require manual adjustments to keep pace with the ever-changing threat landscape.

Challenges of traditional WAFs

### Despite their evolution, WAFs have weaknesses:

**Reactive character:** They react to known threats but are often overwhelmed by zero-day attacks until updates are made available.

**Complexity:** Configuration and maintenance require specialist knowledge, which is a hurdle for smaller companies.

**False positives/negatives:** Rules that are too strict block legitimate traffic, while settings that are too lax allow attacks through.

**Dependence:**

Many WAFs route traffic via external servers, which increases latency and raises data protection issues.

**Danger:**

Can be easily bypassed

# WEBOUNCER: A new era of web security

**WEBOUNCER**, developed by a German company and patented in Europe (EP4430501) and patent pending in USA, is a radical innovation that could potentially replace traditional WAFs. It combines cutting-edge technologies with a fundamentally different approach to overcome the weaknesses of traditional WAFs.

## Here's how **Webouncer will** continue the story:

### Digital twin as a paradigm shift:

#### Concept:

**WEBOUNCER** creates a “virtual copy” of the front end of a web application that is publicly accessible, while the real application and its data remain in a secure data center without any access from the public.

#### Advantage over WAF:

Instead of just filtering traffic, WEBOUNCER minimizes the attack surface from the outset. Attackers interact with a shell without access to sensitive data - a proactive rather than reactive approach.

### Threat detection:

#### Function:

It is analyzed in real time and adapts dynamically to new threat patterns without the need for manual rule updates.

#### Advantage over WAF:

While modern WAFs use machine learning, WEBOUNCER is designed to detect and neutralize threats immediately - no delay due to signature updates.

### CAPTCHA-AI against phishing:

#### Mechanism:

**WEBOUNCER** checks whether requests come from the legitimate domain and blocks access from fake URLs.

#### Advantage over WAF:

Traditional WAFs rarely protect against phishing or website copying. WEBOUNCER adds an additional layer of security that goes beyond pure traffic filtering.

### Simplicity and efficiency:

#### Integration:

**WEBOUNCER** lässt sich ohne komplexe Konfiguration in bestehende Systeme einbinden.

### Advantage over WAF:
Where WAFs often require complex maintenance and expert knowledge, WEBOUNCER offers a plug-and-play solution that is also accessible to smaller companies.

## Privacy and sovereignty:
### Standort:
Data is processed in a GDPR-compliant data center in Germany.

### Advantage over WAF:
Many cloud WAFs store data globally, which harbors legal risks. WEBOUNCER offers a data protection-friendly alternative.

## Independence from DNS redirection:

### Architecture:
**WEBOUNCER** protects the application directly without routing the traffic via external servers.

### Advantage over WAF:
This reduces latency and dependencies, which are a disadvantage with many WAFs.

# How Webouncer will replace WAF

**WEBOUNCER** challenges the evolution of the WAF by shifting the focus from filtering traffic to reducing the attack surface. While WAFs work like a bouncer checking guests against a list, **WEBOUNCER** builds a kind of “deception”: attackers enter a room that is empty while the real data remains securely stored.

### This philosophy could usher in the next level of web security:

### Proactivity instead of reactivity:
**WEBOUNCER** prevents attacks before they cause damage instead of just reacting to them.

### Reduction of complexity:
It eliminates the need for constant rule maintenance, which often makes WAFs impractical.

### Future orientation:
With AI and a digital twin, **WEBOUNCER** addresses modern threats such as phishing or zero-day exploits more effectively.

## Conclusion

The history of WAF is one of constant improvement - from static filters to AI-powered systems. But **Webouncer will** surpass this progress by redefining the basic principles of web security. Instead of filtering traffic, it protects the application itself through isolation and intelligence. For organizations looking for a simple, proactive and privacy-compliant solution, **Webouncer will** indeed herald the end of the traditional WAF era and write a new history of web security.

**WEBOUNCER is currently the only system on the market that is able to pass dynamic content, sessions, cookies, etc. between the source and target system, even if thousands of accesses take place simultaneously.**

# Contact:

We are happy to answer any questions you may have.


Kevin Sweeney
Sales Manager
k.sweeney@kralos.de

Carsten Klein
CEO / co-founder
c.klein@kralos.de


KRALOS