2025

Differences between a Web Application Firewall (WAF) and WEBOUNCER (EP4430501)

FEEL THE DIFFERENCE

CARSTEN KLEIN

KRALOS GMBH | Burgdorf - Germany

Index

Differences between a Web Application Firewall (WAF) and WEBOUNCER

The Web Application Firewall (WAF) and WEBOUNCER are two approaches to protecting web applications from cyber-attacks. While they pursue the same goal - the security of websites and applications - they differ fundamentally in their functionality, philosophy and technology.

Here is a detailed comparison:

1. Basic principle and approach of WAF:

How it works:
A WAF acts as a filter between the internet and the web application. It analyzes incoming data traffic (HTTP/HTTPS) and blocks malicious requests based on rules or patterns.

Approach:
Reactive - it detects and blocks known threats such as SQL injection, XSS or DDoS attacks according to predefined criteria.

Example: A WAF stops a request that contains suspicious code, e.g. `<script>alert('XSS')</script>`.

1.1 Basic principle and approach of WEBOUNCER:

How it works:
WEBOUNCER uses a “digital twin” - a publicly accessible copy of the front end - while the actual application and sensitive data run in an isolated data center.

Approach:
Proactive - instead of just filtering traffic, WEBOUNCER reduces the attack surface by allowing attackers to interact only with a data-less shell.

Example:
An attacker attempting an SQL injection only reaches the copy and cannot manipulate any real data.

2. Technological differences WAF:

Technology:
Rule-based filters (signatures), partly supplemented by machine learning for anomaly detection.

Deployment:
Often runs as a reverse proxy that redirects traffic via its own servers (cloud WAFs such as Cloudflare) or locally as an appliance.

Dependency:
Requires regular updates to rules/signatures to defend against new threats.

2.1 Technological differences WEBOUNCER:

Technology:
Combination of digital twin, AI-based threat detection and CAPTCHA-AI for domain validation.

Deployment:
Works directly with the application without necessarily redirecting traffic via external servers.

Dependency:
Adapts dynamically to new threats without manual updates.

3. Protection mechanism WAF:

Protection:
Blocks malicious traffic by “blacklisting” (known threats) or “whitelisting” (only permitted traffic).

Limitations:
Can fail in zero-day attacks until a new rule is created.
Does not actively protect against phishing or website copies.

Attack surface:
The application itself remains potentially vulnerable if the WAF is bypassed.

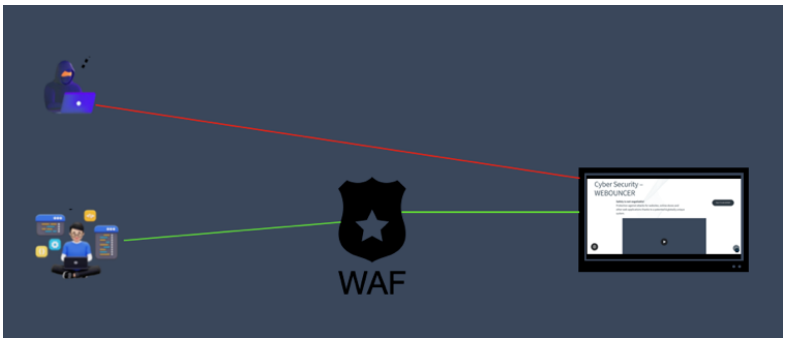


Fig.: Shows bypass of a WAF

3.1 Protection mechanism WEBOUNCER:

Protection:
Prevents attacks by separating sensitive data and logic from the public interface. The AI detects anomalies in real time.

Strength:
Also protects against phishing by checking domain authenticity and minimizes the attack surface through the digital twin.

Attack surface:
Drastically reduced, as attackers only encounter an empty shell.

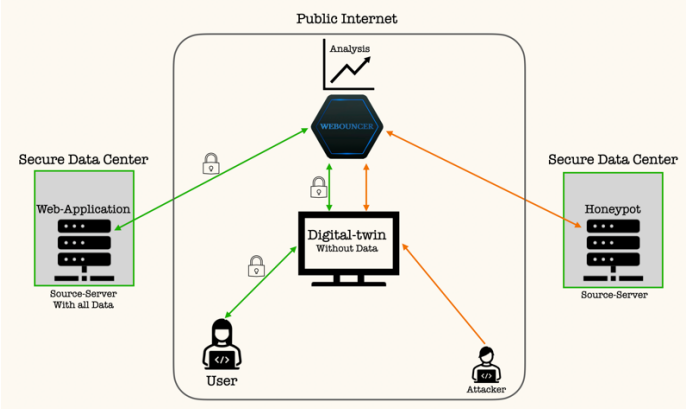


Fig.: Shows how WEBOUNCER works

4. Complexity and management WAF:

Setup:
Often requires complex configuration (rules, policies) and regular maintenance.

Administration:
Expertise needed to minimize false positives (legitimate users blocked) or false negatives (attacks allowed through).

Costs:
Higher due to maintenance costs and subscriptions for cloud WAFs.

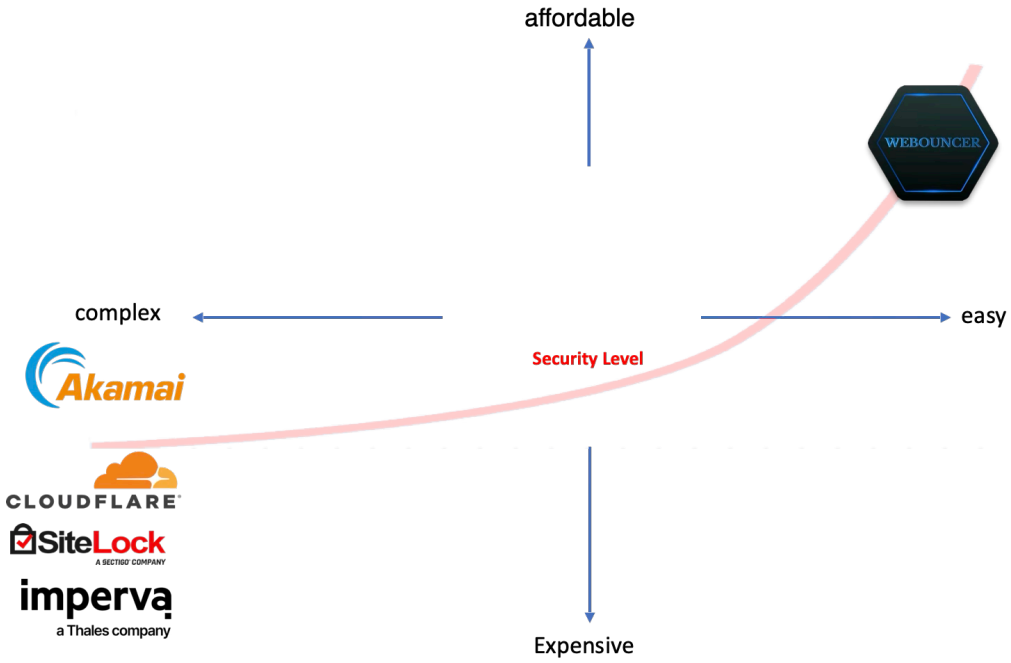
4.1 Complexity and management WEBOUNCER:

Setup:
Simple integration into existing systems without complex rules and regulations.

Management:
Automated by AI, little to no manual intervention required.

Costs:
More cost-efficient due to lower administrative costs.

Overview of costs / security level



5. Data protection and location WAF:

Data processing:
Often globally distributed in the case of cloud WAFs, which can raise data protection issues (e.g. GDPR).

Location:
Depends on the provider, often outside the EU.

5.1 Data protection and location WEBOUNCER:

Data processing:
Runs in a highly secure, GDPR-compliant data center in the EU.

Location:
Guarantees EU data protection standards.

6. Latency and performance WAF:

Effect:
Can increase latency as traffic is routed via proxy servers.

Performance:
Depends on the configuration and load.

6.1 Latency and performance WEBOUNCER:

Impact:
Minimizes latency, as no redirection via external servers is necessary.

Performance:
Optimized through direct architecture.

7. Example scenario WAF:

A hacker attempts an SQL injection. The WAF recognizes the pattern (e.g. `1=1`) and blocks the request, but a new, unknown pattern could get through.

7.1 Example scenario WEBOUNCER:

The same hacker attacks the public copy. Since there is no database behind it, the attack has no effect and the anomaly is registered.

Table: Overview of the differences

Kriterium	WAF	WEBOUNCER
Approach	Reactive (traffic filtering)	Proactive (reduce attack surface)
Technology	Rules, partly AI	Digital twin, AI, Captcha-AI
Protection	Known threats	New threats, phishing
Complexity	High (regular maintenance necessary)	Low (automated)
Privacy	Provider-dependent	GDPR-compliant (GE, EU)
Latenz	Potentially increased	Minimal

Conclusion

A WAF is a proven tool that monitors data traffic like a bouncer, but it remains reactive and complex.

WEBOUNCER, on the other hand, revolutionizes protection by securing the application itself - through a digital twin and AI - preventing attacks before they can cause damage. For companies looking for a simple, future-proof and data protection-friendly solution, WEBOUNCER could not only complement the WAF, but also replace it in the long term.

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

WEBOUNCER (EP4430501) 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.