2025

Guide to the security of web-based applications and the benefits of WEBOUNCER

THE ADVANTAGES OF WEBOUNCER

CARSTEN KLEIN

KRALOS GMBH | 31303 Burgdorf - Germany

Index

The security of web-based applications is crucial to protect data, users and your company from cyberattacks. In this guide, you'll learn how to make your web application secure and discover the benefits of WEBOUNCER - an innovative solution that outperforms traditional security approaches. Whether you're a developer, business owner or IT manager, you'll find practical tips and a modern alternative for maximum protection.

1. Understanding the basics of web security

Cyber attacks such as SQL injection, cross-site scripting (XSS), DDoS attacks or phishing are everyday threats to web applications. To minimize these risks, start with these essential measures:

- Use HTTPS: Encrypt data with SSL/TLS certificates (e.g. via Let's Encrypt).
- Check inputs: Validate and clean user data to prevent injections (e.g. with prepared statements).
- Strengthen authentication: Use two-factor authentication (2FA) and complex passwords.
- Install updates: Keep software, frameworks and libraries up to date.

Tip: Analyze vulnerabilities regularly with tools such as OWASP ZAP.

2. Embedding security in the development process

Secure development is the first step towards a robust application:

- Secure coding: Avoid insecure practices such as direct execution of user data (see OWASP Top 10).

- Code reviews: Have your code checked to detect errors early on.

- Automated tests: Use tools such as Snyk or SonarQube for security analyses.

Practical example: Integrate security checks into your CI/CD process to find vulnerabilities automatically.

3. Protection against advanced threats

Modern attacks require more than just basic measures:

- Web Application Firewall (WAF): Filter malicious traffic - but many traditional WAFs are complex and reactive.

- Content Security Policy (CSP): Restricts which resources may be loaded in order to stop XSS.

- Rate limiting: Limit requests to ward off DDoS or brute force attacks.

Tip: Use a reverse proxy like NGINX with `limit_req` to control traffic.

4. Data protection and legal security

Data protection is a must - both technically and legally:

- Comply with the GDPR: Obtain consent and store data securely.

- Encryption: Use AES-256 for data at rest and TLS for transmission.

- Backups: Create regular, encrypted backups.

Tip: Choose servers in the EU (e.g. Germany) to simplify legal requirements.

5. The limits of traditional solutions

Conventional security solutions such as WAFs have weaknesses:

- Reactive approach: They only block known threats and require constant updates.

- Complexity: Complex configuration and maintenance increase costs and sources of error.

- Limited protection: They often do not protect against phishing or new attack patterns.

This is where WEBOUNCER comes in - an innovative alternative that closes these gaps.

6. The advantages of WEBOUNCER

WEBOUNCER takes the security of web applications to a new level. Here are the main advantages:

- Digital twin: The public front end is provided as a data-free copy, while the actual application with sensitive data runs in a secure data center.
This drastically reduces the attack surface.

- Advantage: Attackers only interact with a shell, without access to real data.

- Proactive AI: WEBOUNCER recognizes threats in real time and adapts dynamically to new attack patterns - without constant rule updates.

- Advantage: Faster protection than with reactive WAFs.

- CAPTCHA-AI: An AI checks whether access comes from the legitimate domain and thus protects against phishing or website copies.

- Advantage: Additional security against identity theft.

- Simplicity: No complex configurations - WEBOUNCER is easy to integrate into existing systems.

- Advantage: Saves time and costs compared to traditional WAFs.

- Data protection: Data is processed in a GDPR-compliant data center in Germany.

- Advantage: Ideal for companies with strict legal requirements.

- Independence: Works without DNS redirection or external server dependencies.

- Advantage: More control and flexibility.

Practical example: An e-commerce company uses WEBOUNCER to protect customer data. Phishing attacks fail due to AI validation, while the digital twin technology seals off sensitive data.

7. WEBOUNCER in practice

- Integration: Add WEBOUNCER to your infrastructure - no extensive conversion required.

- Test phase: Start with a demo to experience the protection live.

- Scaling: Use it for small websites or complex applications alike.

Tip: Combine WEBOUNCER with CSP and rate limiting for all-round protection.

Conclusion

Web application security requires a mix of best practices and modern solutions. While basic measures such as HTTPS and input validation are essential, WEBOUNCER offers a decisive advantage: it protects proactively, reduces the attack surface and is easy to use. For companies that value efficiency, data protection and innovation, WEBOUNCER is a smart alternative to conventional security solutions.

WEBOUNCER is like an invisible bouncer: only legitimate visitors get in, while attackers are faced with an empty shell.

We are happy to answer any questions you may have.
Contact:

Kevin Sweeney
Sales Manager
k.sweeney@kralos.de

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

KRALOS