radware

Adapt and Neutralize

7 Characteristics a WAF Should Provide

SQL injections, cross-site scripting, illegal resource access, remote file inclusion…the tools available to hackers attacking web applications are as diverse as the infrastructure and services that web application firewalls (WAF) are required to protect.

Businesses require a next-generation WAF that is flexible enough to adapt to changing IT infrastructures and the evolving threat landscape, and also change based on the needs of the business. Here are 7 characteristics to look for when considering a WAF offering.

1. Agility Equals Security Risks – DevOps and agile development practices are great at creating new applications quickly and efficiently. Unfortunately, the fluidity of these environments also creates a bevy of unintended security risks. Ensure any WAF solution **can automatically detect and protect applications** as they are added to the network by automatically creating new policies and procedures.

2. Cover That Top Ten List – Industry pundits and experts at security consortiums and communities continue to categorize and identify the greatest web application security risks facing organizations. A WAF solution should provide complete coverage, including all **OWASP Top 10 risks**.

3. Device Fingerprinting – Bots, crawlers and spammers, using new techniques to disguise malicious traffic, can exhaust resources and scrape sensitive information from websites or cloud-based assets. A good WAF needs to sniff out these clandestine cyber assaulters. **Device fingerprinting** identifies, blacklists and blocks machines used for attacks regardless of the IP they hide behind. Even if the bot dynamically changes its source IP address, its device fingerprint does not change.

4. Negative + Positive = Zero-Day Protection – Advanced application and "smoke screen" attacks that use DDoS assaults to mask other tactics are becoming commonplace, while zero-day assaults swiftly exploit newly discovered vulnerabilities. **Negative and positive security models** that automatically detect application domains, analyze potential vulnerabilities, and assign optimal protection policies are critical.

5. Who's Knocking at the Door? – Enforcing web access control policies and security procedures is a bread and butter function of any WAF. How to do it is where the devil is in the detail. Ensure any WAF offering supports **user authentication and single sign-on (SSO) functions**. This applies two-factor authentication and enables access to premise-based applications from outside the enterprise network. In addition, it ensures access to data based on a user's role/business needs.

6. Two Minds Are Better Than One – Cyber-attacks are increasing in severity and complexity, making it difficult for organizations to stay ahead of the rapidly evolving threat landscape. To assist, a WAF vendor should provide options for **fully managed services** for both on-premises and cloud-based WAF deployments. This provides the organization with the insight and expertise from security experts that can assume full responsibility to configure and update security policies as well as actively monitor, detect, alert and mitigate attacks in real time.

7. Protection Via Unification – Leading analysts agree that the best WAF solution is one that provides both **on-premises and cloud-based offerings**. It provides a unified solution that ensures complete availability and protection with no security gaps between on-premises and web applications, and facilitates quick and easy migration of applications to the cloud.

Select a WAF solution that provides complete coverage while adapting to your changing IT environment. Learn more about Radware's AppWall and Cloud WAF Service.