radware

7 Capabilities Every Web Application Firewall Should Provide

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

Businesses require a WAF that can provide complete coverage while adapting to your changing application environment. **Here are 7 characteristics to look for when evaluating a WAF.**

1 Agility Equals Security Risks

DevOps and agile development practices are great at developing and deploying new application 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 have become commonplace, and zero-day assaults swiftly exploit newly discovered vulnerabilities. **A WAF that employs both negative and positive security models to automatically detect application domains, analyze potential vulnerabilities,** and assign optimal protection policies is 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

Cyberattacks 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-premise 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-premise and cloud-based offerings.** It provides a unified solution that ensures complete availability and protection with no security gaps between on-premise and web applications and facilitates quick and easy migration of applications to the cloud.

Learn More About What Comprehensive Application Protection Looks Like

READ ABOUT RADWARE SOLUTIONS HERE

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware’s solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit radware.com.

Radware encourages you to join our community and follow us on: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.