Choosing a WAF

Balancing False Positives and Negatives

Akamai
FASTER FORWARD

Organizations purchasing a Web Application Firewall (WAF) often do not understand the potential impact of false positive and false negative outcomes. Couple this with misleading accuracy metrics from vendors, and the result? Organizations often buy WAFs that soon must be disabled or taken out of line to avoid severe impact on the site because they are allowing malicious traffic through. You can avoid this fate.

What is WAF accuracy?

Accuracy measures the ability of a WAF to not only stop web attacks but to also allow through all legitimate users. Here we'll focus on the two undesirable metrics:

- **False positives (FP) –** legitimate user requests that are improperly identified as an attack and therefore blocked by the WAF
- **False negatives (FN) –** real attacks that are not identified and blocked by the WAF and are passed through to the application

Comparing Vendor Claims

Accuracy numbers can only be compared if they come from the same test. For example, let's say vendor 1 protects against 10 attack vectors. They run a test, catch all of them, and claim 100% accuracy. Looking good, right?

Now, let's say vendor 2 protects against 100 attack vectors – 10 times as many as vendor 1. They run a different test, catch the same 10 vectors plus another 80 vectors, but they miss the last 10. They are only 90% accurate. Which vendor would you rather have protecting you?

Tension Between False Positives and False Negatives

Some WAF vendors tune their firewalls for low false positives. It makes sense, except that often comes at the expense of false negatives, which is dangerous. Why? Because a false negative is a web attack that the solution didn't catch and passed through to the application.

So a vendor claiming really low false positives, but saying nothing about false negatives, should be a real concern. Their false negatives are probably too high to talk about.

Why Zero is Not the Best Number

It's really easy for a web security solution to have 0% false positives — all they have to do is turn off all security controls and allow all traffic through. They'll never accidentally block legitimate users, because they aren't blocking anything.

Conversely, it's also really easy for any web security solution to have 0% false negatives. Just block everything, including legitimate users.

Of course, neither approach leads to a very effective web security solution. That's why we need to talk about false positives and false negatives together.

Do You Have to Make a Trade-Off?

There is a tension present in any WAF solution – the risk of misidentifying legitimate traffic as an attack vs. failure to identify malicious web traffic.

WAF solutions have historically required organizations to make a trade-off between false positives and false negatives – by minimizing false positives at the expense of allowing malicious traffic. While this may alleviate your concerns about blocking legitimate users, it also protects against fewer web attacks.

Akamai offers a more effective approach to lower rates of both false positives and false negatives. We can increase the accuracy of your WAF protection while minimizing impact on legitimate users.

Akamai's Approach to WAF

The Akamai WAF solution takes a different approach from many traditional WAF solutions. The Kona Rule Set (KRS) employs a small number of flexible rules in conjunction with an anomaly scoring model for improved accuracy.

Broader and More Flexible Rules

Rather than address each vulnerability with a dedicated rule, KRS utilizes a smaller number of broader but more flexible rules to identify malicious requests. Each rule detects an attribute shared by multiple vulnerabilities. Combinations of rule triggers can often be observed during web attacks.

Multiple rules identify an attack. Rules vary in their accuracy, so we deliver better accuracy by requiring them to work together. For example, one rule may be prone to false positives on its own but is indicative of an attack when triggered with another rule.

Weighted Risk Scoring

Triggered rules contribute to a weighted risk score that reflects the accuracy of each of the individual rules and the contribution of each rule in identifying the anomaly. KRS alerts on or blocks a request if the cumulative risk score for that request exceeds the defined threshold for the relevant category.

This approach results in greater accuracy. It also increases the likelihood of catching new attack permutations (zero day attacks) with existing rules. And it results in less operational overhead to manage Akamai's WAF solution over time.

Tuning the Rule Set with Automated Testing

Real world traffic is needed to test a WAF's response. Akamai web security teams have a deep understanding of the characteristics of legitimate and malicious traffic. Every day, our CDN platform delivers both legitimate and malicious HTTP requests – including requests prone to produce false positives and false negatives.

Akamai uses this data to perform closed-loop testing to measure the accuracy of KRS and identify sources of false positives and false negatives.

The Right Balance Between False Positives and False Negatives

Automated testing allows Akamai to better understand how changes to KRS impact overall accuracy and to fine-tune score weightings for the optimum balance between false positives and false negatives.

For example, examining false negatives may reveal probes that pose low risk but closely resemble legitimate requests. Tuning KRS to identify these requests as malicious would not be in users' best interests if it blocked legitimate traffic. In this case, the benefit of a lower false positive rate outweighs that of slightly higher false negatives.

While we tune for the best WAF for the vast majority of our customers, Akamai also ensures your ability to tune KRS for your specific environment, such as to remove these false negatives, if desired.

Next Step: Learn More About Akamai's Approach to WAF

Learn more about Akamai's approach to WAF in the white paper Improving Web Application Security: The Akamai Approach to WAF.