7 Questions to Ask Before Buying a Web Application Firewall

Akamai
FASTER FORWARD

1. How much throughput do I need?

A Web Application Firewall (WAF) protects your website or web application by inspecting each HTTP and HTTPS request. In many cases, the inspection protects you from data loss, web defacement, or worse – an attacker gaining control of your web server. But that inspection comes at a cost: latency. And the lower your WAF's throughput, the more potential latency. In other words, if the size of a web application attack (or even spikes in legitimate traffic) exceeds the throughput of the web application firewall, the web application firewall can slow down incoming requests. Even worse, if the WAF is completely overwhelmed with requests, it could fail and either no longer inspect the requests coming to your application (fail open) or block traffic altogether (fail close). Purpose-built, on-premise WAFs generally top out at 2 Gbps of throughput. Cloud-based WAFs can carry an order of magnitude (or even two) more than that.

2. How much visibility into new attacks does my WAF have?

The more attacks a WAF solution and vendor observes, the more it will learn about attack patterns, attack payloads and attack characteristics. Does your WAF vendor collect data? From where? How often is the data updated? And how is the data used to improve your protection? Generally purpose-built, on-premises WAFs can only process the data coming to the websites and web applications they protect. Some on-premises WAF vendors buy threat feeds from third parties, while others rely on their customers to opt in to data sharing. Knowing where your vendor's data originates will help you assess the quality of your vendor's WAF.

3. How does my WAF vendor acquire intelligence?

Data is required to build intelligence, but data does not necessarily equal intelligence. How is the data stored, queried and used? How does your vendor use that data to improve protection? Does your vendor have a closed-loop test framework to feed data into your WAF? Is the data used to tune WAF rules? Asking your vendor how data is turned into intelligence will reveal their quality assurance practices and help you understand whether the WAF is static or dynamically adjusts to attack trends.

4. Who will manage my WAF?

Cloud-based WAFs lend themselves to management by partners or third-party teams. Most companies that purchase cloud-based WAFs elect to partner with the WAF vendor to manage the WAF. Cloud-based WAFs typically include an HTML-based graphical user interface (GUI) configure rules, track traffic, update white and black lists, and conduct other management tasks. On-premise WAF vendors, meanwhile, typically are only sell hardware and do not offer services for long-term management of their solution. Companies that purchase on-premises WAFs will require a full-time employee (FTE) to configure, manage and update the rules – and to stay on top of new attacks and trends. Consider the cost of hiring an FTE in your calculation of the total cost of ownership of your WAF.

5. What is the false negative rate on my WAF?

No WAF is 100 percent accurate, and no WAF is foolproof. One useful measurement of accuracy is the false negative rate. This number reflects the malicious requests that are not caught by the WAF and make it through to the website or web application. The higher your WAFs false negative rate, the more malicious requests are likely to get through. Ask your vendor how they measure false negatives, and what the false negative rate is for their most recent model or software version. Understand whether false negatives are improving over time by asking about false negative rates for previous models or versions.

6. What is the false positive rate on my WAF?

Similar to the false negative rate another useful measurement is the false positive rate. This tracks legitimate user requests that are erroneously flagged by as malicious. The higher the false positive rate of your WAF, the more legitimate user traffic is likely to be erroneously blocked. Ask your vendor how they measure false positives, and what the false positive rate is for its product.

WAFs with a low false negative rate, (stricter WAFs) will typically have a higher false positive rate, and vice versa: WAFs with low false positive rates typically have a higher false negative rate. Most WAF solutions require you to make this tradeoff. You may have to decide whether you can more readily tolerate blocked users (i.e., paying customers) or unblocked attacks.

7. Does your WAF include rate controls, brute force protection, and DDoS mitigation?

Today's cloud-based WAFs frequently include some measure of DDoS mitigation capability, rate controls, and/or protection against brute force logins. This is in response to a trend among attackers to use multi-vector attacks. Many attackers will wait for a publicized DDoS attack, or launch a DDoS attack themselves, and then sneak in with a web application attack designed to steal data. Understand if your WAF vendor offers these services. If they do not, evaluate your DDoS mitigation posture and include the cost of updating your DDoS protection with your WAF purchase.