Securing your web applications can be a daunting task, especially without dedicated security staff or training. A web application firewall (WAF) keeps threats at bay while preserving application performance. But with so many solutions out there, selecting one is not so simple. Let’s dispel some WAF myths that will help you evaluate what matters most — so you can worry less about attacks, and more about growing your business.

**MYTH 1:** Operating a WAF is complicated.

It shouldn’t be. The Akamai WAF simplifies distributed denial-of-service (DDoS) and application-layer security with rule sets that are easy to manage. WAF rules are automatically updated to protect against the latest cybersecurity threats, so your defenses always stay current. Rules are thoroughly tested to keep threats out and legitimate users in, without any surprises. And if you’re ever in need of security expertise, Akamai provides 24/7/365 access to support.

**MYTH 2:** More customizable rules deliver more security.

When it comes to ease of use, less is more. Having more rules to customize causes unnecessary complexity, especially if your organization doesn’t have the security expertise on staff to dive into the details of rule dependencies and interactions. Akamai’s automated WAF rule sets are bundled into eight categories — all you have to do is turn them on. With fewer dials to adjust, you’re less likely to cause a problem when you tweak them.

**MYTH 3:** Outages are just a cost of doing business.

Outages are no longer an acceptable part of doing business online. *Network World* reports that one hour of downtime can cost small companies as much as $8,000 and midsize companies up to $74,000. Providing scale and resiliency with 100% availability in over 130 countries and across more than 1,700 networks around the world, Akamai is trusted by the most availability-sensitive industries, including eight of the top global FinTech firms and 91 of the top U.S. Internet retailers.
MYTH 4: **Faster rule updates provide faster application defense.**

Not if those rules aren’t properly vetted. When rushed into production, new WAF rules can have the opposite effect. To protect our customers, Akamai tests new rules in two phases: first, in our lab against known legitimate and malicious traffic; then, on the platform to analyze the change for false positives and false negatives against live Internet traffic. Don’t trade speed for quality by letting your business experiment with new rules.

---

MYTH 5: **Crowdsourced threat analysis provides enough protection.**

Analysis that depends solely on crowdsourcing lacks precision, validation, and context for the behavior — and doesn’t account for false positives. Delivering more than 95 exabytes of data across billions of devices for over 6,000 of the largest online companies, Akamai has tremendous visibility into huge quantities of legitimate and malicious traffic around the world and across industries. By observing this traffic, Akamai security experts can see how attacks and legitimate traffic evolve. This insight benefits rule accuracy across all industries.

---

MYTH 6: **A higher number of rule triggers indicates better results.**

The number of rule triggers is just the noise of the machine. What really matters is the correlation and scoring of triggers that result in the number of attacks the WAF detects. Akamai delivers more than 2 trillion Internet interactions and interacts with more than 100 million IP addresses every day, which gives us unmatched intelligence and insight. Most attacks start in one industry before moving to others. With hundreds of millions of web attacks across multiple verticals observed each week, Akamai’s unique perspective helps you stay ahead of threats and protected from cyberattacks before they spread.

---

MYTH 7: **You don’t need to protect your APIs.**

In an ever-more-connected digital world, it’s not enough to protect your web pages. Proper API security reduces your attack surface. The Akamai WAF can protect APIs against DDoS and web application attacks by blocking API traffic based on IP address, geolocation, abnormal access, or an excessive rate of requests. The Akamai WAF automatically inspects API requests (including JSON and XML) for malicious content, extending a high level of protection from websites to APIs.
**MYTH 8: A WAF can protect against all zero-day attacks.**

By definition, a zero-day attack isn’t known yet, so no vendor can make that promise – but that doesn’t mean a WAF can’t help here. For example, the Akamai WAF uses anomaly-based rules to spot zero-day attacks that share similarities to known cases. Architected as an anomaly scoring mechanism, the Akamai WAF has detected attacks exploiting zero-day vulnerabilities without any additional tuning required. Also, Akamai WAF rules update automatically, so you don’t have to keep up with the constantly changing threat landscape.

---

**MYTH 9: A WAF mitigates all bots.**

While a WAF provides an important layer of protection against bots, the Akamai WAF blocks known bots and those that are sending a lot of traffic. Left unattended, noisy bots bog down systems and impact legitimate traffic. A WAF is an easy way to manage bots that drain resources without causing any other harm. If more sophisticated bot operators target an organization, they will find a way around the WAF. For those cases, Akamai also offers specialized bot management solutions that detect and protect against advanced bot threats like credential theft.

---

**MYTH 10: Individual point solutions are superior in their areas of specialization.**

When it comes to protecting against the latest cybersecurity threats, the knowledge transfer that comes with a breadth of security offerings – and the volume of incidents observed along with them – creates more effective automated protection, better anomaly detection, and higher-quality rule sets. A security strategy that uses point solutions from multiple vendors is often more difficult to manage, requires more training, and poses integration challenges.

---

To learn more about how Akamai WAF can make security easier for you with application-layer and DDoS protection, visit Akamai.com/Security.

---

Akamai secures and delivers digital experiences for the world’s largest companies. Akamai’s intelligent edge platform surrounds everything, from the enterprise to the cloud, so customers and their businesses can be fast, smart, and secure. Top brands globally rely on Akamai to help them realize competitive advantage through agile solutions that extend the power of their multi-cloud architectures. Akamai keeps decisions, apps, and experiences closer to users than anyone – and attacks and threats far away. Akamai’s portfolio of edge security, web and mobile performance, enterprise access, and video delivery solutions is supported by unmatched customer service, analytics, and 24/7/365 monitoring. To learn why the world’s top brands trust Akamai, visit akamai.com, blogs.akamai.com, or @Akamai on Twitter. You can find our global contact information at akamai.com/locations. Published 04/19.