Akamai

PAPER

Simplify Your Web Application Security

Web Application Attacks

Modern web applications have become complex, especially with the increasing adoption of microservices-based architectures. Heavy reliance on APIs for virtually every online interaction contributes to this complexity and brings with it the potential for new entry points for hackers. Known web vulnerabilities, meanwhile, continue to live on and are reintroduced into applications by each new generation of coders. Today's attackers have evolved in response by using bots, distributed denial of service (DDoS) for hire, and multivector attacks to target web applications, APIs, and even client-side vulnerabilities.

Opportunistic attacks, however, are still the most common form of web attack – they don't set out to target your organization, but will do so after discovering a vulnerability. Scanners use automated bots to crawl websites at random, constantly looking for any of thousands of vulnerabilities. Once a vulnerability is found, attackers can make a database reveal its secrets, load malicious files onto a web server, or hammer a site with an overwhelming burst of traffic.

What Are the Risks Associated with Web Attacks?

Organizations with low risk tolerance need high security outcomes to build a chain of trust – both internally (e.g., among systems, supply chain, operations, etc.) and externally (e.g., with partners, customers, governing bodies, etc.). APIs in particular – from simple internal flows among parts of a microservice application to major business-to-business transactions – are especially important to secure because they serve as the digital glue that connects various systems and partner ecosystems and enables digital and omnichannel customer experiences.

Cybercriminals, unfortunately, have an almost limitless arsenal of web attack methods designed to cause maximum damage. A successful hack that results in the exfiltration of sensitive data or a DDoS attack that renders your sites unavailable can break this trust and cause significant harm from loss of customer loyalty, regulatory fines, lawsuits, and diminished brand reputation.

Challenges with Web Application Security

Cloud-based web application and API protection (WAAP) solutions are designed to mitigate many forms of web application, DDoS, and API-based attacks. One of the primary challenges with firewalls, however, is that AppSec teams must constantly analyze and tune rules as applications change, threats evolve, and updates become available. This is often a time-consuming manual process that requires skilled operators and is unscalable for most organizations.

Outdated security policies can become the source of frustration as alert fatigue drastically diminishes the ability to accurately differentiate false positives from real attacks. Security teams that are unable to tune rules effectively may also pull their protections out of line and knowingly accept a heightened risk posture for fear of impacting legitimate users and disrupting business.

Why Akamai WAAP?

Akamai App & API Protector is a cloud-based WAAP solution — including bot visibility and mitigation — that is designed to protect your applications and APIs from a wide range of network and application layer threats with less effort and overhead. From a self-service onboarding wizard, which easily integrates and configures workflows, to self-tuning recommendations that automatically analyze triggers to apply exceptions, App & API Protector removes many of today's firewall issues that are a source of intraorganizational friction and an obstruction to deployment.

Automated protections — fully managed by Akamai — then allow you to take a completely hands-off approach to web application security. Automatic protection from web attacks like SQL injection, cross-site scripting, and local file inclusion provide broad coverage with virtually no ongoing maintenance. And by applying machine learning and heuristics, we accurately identify false positive patterns across your traffic on a policy-by-policy basis — not a generic network-wide check — for the most relevant and actionable results.

Raising the Bar with Adaptive Protections

So, how does Akamai App & API Protector deliver both simplicity and accuracy? First, Akamai's adaptive security engine takes into account all data points and assigns a threat score to each request. The higher the threat score, the more aggressive the protections — and by dynamically modifying protections to fit the level of detected threat, we can identify even the most evasive attacks while keeping false positives ultra low.

Web application attacks usually involve some form of reconnaissance, but as attackers scan for vulnerabilities, Akamai builds evidence about their techniques and tactics. This not only makes them immediately identifiable, but it leaves behind a historical fingerprint for your specific traffic should they return. The more often an attacker tries, the stronger your protections get.

Akamai has insight into:

16.8 million+
daily web application attacks

12 billion
bot requests

280 million
bot logins

Crowdsourced Threat Intelligence

Many of the most-attacked websites on the internet are Akamai customers, including 850 of the largest retailers, 300 of the world's largest banks, more than 950 enterprise hardware and software companies, and over 200 national government agencies. We have visibility into more than 16.8 million daily web application attacks, 12 billion bot requests, and over 280 million bot logins. More than 330 industry-recognized threat researchers and data scientists at Akamai query over 303 TB of new attack data daily for threats. This level of insight, coupled with advanced machine learning and human analysis, allows us to proactively and predictively stop both common and highly sophisticated attacks.

Akamai has mitigated web application attacks for more than a decade and has protected customers and maintained infrastructure availability while withstanding some of the largest attacks. We continue to investigate and report on emerging threats, and as attacks continue to evolve and grow larger and more sophisticated, we continue to innovate and adapt our solutions to stay ahead of those with malicious intent. And since App & API Protector is built on the Akamai Intelligent Edge Platform, it comes pre-built with performance capabilities that are designed to ensure your websites, web applications, and APIs perform their very best.

Review Your Web Application and API Protection Needs

If you would like Akamai's help in reviewing and reducing the risk to your websites and web applications, please **contact us**.