Akamai

WHITE 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 multi-vector 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 (among systems, supply chain, operations, etc.) and externally (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.

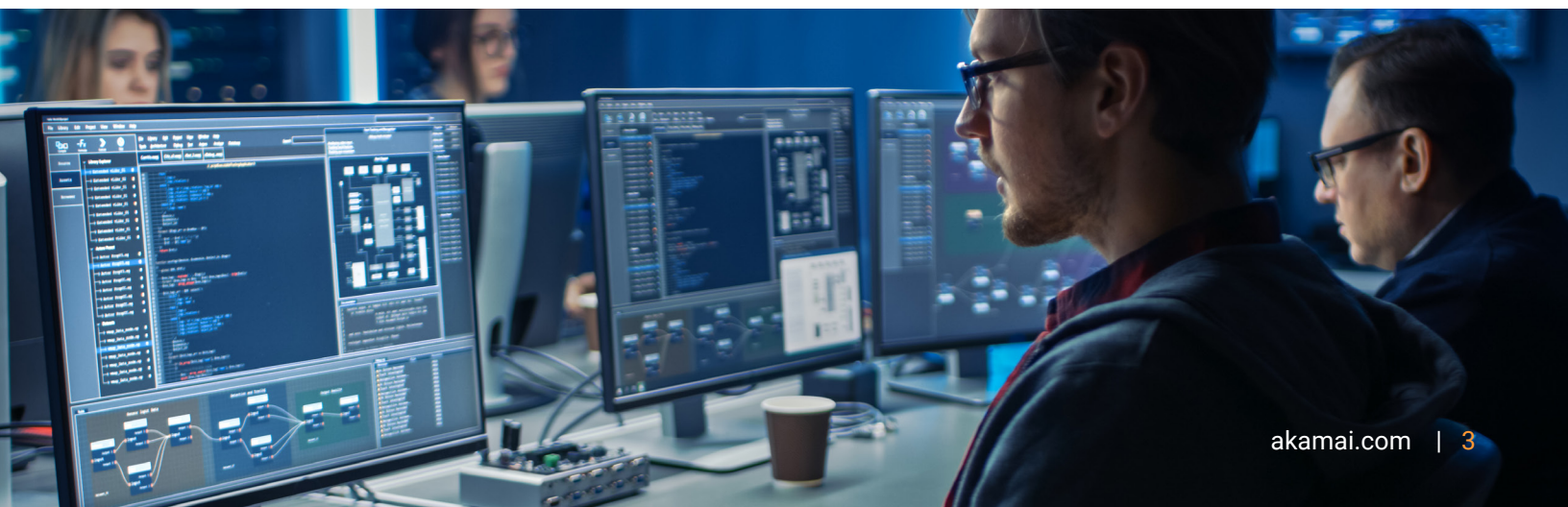
Challenges with web application security

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. Staffing of experienced security professionals remains a challenge, with skilled people often moving roles every two years. This is often a time-consuming manual process that requires skilled operators and is unscalable for most organizations due to turnover, learning lifecycles, and specialized technology integration architectures.

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 at scale from a wide range of network and application-layer threats with less effort and overhead. Akamai's self-service onboarding wizard reduces the need for prior knowledge, providing guidance and insights to quickly and easily secure your assets. Our automated setup process will analyze security triggers and learn the applications' behavior to self-tune protections — leading to more resource savings. App & API Protector removes many of today's firewall issues that are a source of intraorganizational friction, operational weight, and deployment obstruction.



Automated protections — capable of being fully managed by Akamai — are enforced on the world's most distributed platform, then allow you to take a hands-off approach to application security and API protections. 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 are able to enhance identification of 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.

Validate your security stance with our CVE lookup tool, which provides detailed information per CVEs, including threat levels and insights into Akamai's current protections, to help guide your internal security and development strategies. Plus, improve alignment internally and speed time to market with Akamai's pre-built SecDevOps integrations, including Akamai as code, APIs, CLI, Terraform, and integrations.

Raising the bar with adaptive protections

So, how does Akamai App & API Protector deliver both simplicity and accuracy? First, Akamai Adaptive Security Engine, the core technology in App & API Protector, is unique because it learns traffic and attack patterns unique to each customer, analyzes the characteristics of every request in real time, and uses that knowledge to intercept and adapt to future threats. This technology eases security operations by taking into account all anomalous or suspicious data points and assigning 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.

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 it possible for high-tempo identification, but it leaves behind a historical fingerprint for your specific traffic, should the attackers return. The more often an attacker tries, the stronger your protections get.

Akamai has insight into:

780+ million
daily web application attack alerts

26+ billion
bot requests

932+ TB
daily data analyzed

Crowdsourced threat intelligence

Many of the most-attacked websites on the internet are Akamai customers, including 9 of the top 10 retail companies, all top 10 banks, 9 of the top 10 healthcare companies, all 6 U.S. military branches, and the list goes on. We have visibility into more than 780 million daily web application attacks and 26 billion bot requests. Hundreds of expert threat researchers and data scientists at Akamai query over 932 TB of new data daily for threats. This level of global insight — coupled with advanced machine learning, AI, and human analysis — allows us to proactively and predictively stop both common and highly sophisticated attacks.

Akamai has mitigated 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 platform, it comes pre-built with performance capabilities that are designed to ensure your websites, applications, and APIs perform at their very best.

Review your web application and API protection needs, and discover the benefits of Akamai App & API Protector by using this free trial.

Akamai protects your customer experience, workforce, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's cloud computing, security, and content delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn. Published 06/24.