Akamai

WHITE PAPER

From WAF to WAAP: Akamai’s Approach to a Holistic App and API Security Solution

Contents

Introduction

With increasingly large and diverse attack surfaces, growing operational friction and cost, and continuously evasive multidimensional threats, security teams need visibility beyond the traditional web application firewall (WAF). Specifically, they need more automated tools to increase efficiency, and deeper protections in the app and application programming interface (API) ecosystem. The more modern terminology for these protections is web application and API protection (WAAP). Discerning organizations prioritizing the security of their business and the safety of their customers demand comprehensive protection against several threats across their entire digital estate. In addition to protecting apps from known, unknown, and zero-day attacks, these protections include:

- Adaptive threat detection
- Automated policy updates
- Robust DDoS defense
- API discovery and protection
- Bot visibility and mitigation
- Easy integrations for development lifecycles

This paper discusses the traditional WAF technology, the shift from WAF to WAAP, and the continued market demand that is evolving WAAP solutions. As an established leader in the security space, Akamai focuses our approach on innovating security technologies that power and protect life online for end users.

Traditional definition of a WAF

A traditional WAF sits in the middle of the traffic flow between end users and a web application. The WAF inspects unencrypted or encrypted HTTP traffic passing through it for any attacks as defined by a list of rules.

Most WAFs rely on a predefined list of rules to identify malicious HTTP requests interspersed with legitimate HTTP traffic to guard against thousands of potential known exploits. In addition, new attack vectors or additional permutations of existing ones continuously evolve and are exploited by threat actors. This is where a traditional WAF continually needs to have its rules updated and tuned to the legitimate traffic characteristics, which will differ on a per-application basis and change over time.

As end users have demanded more protection and performance, WAFs have expanded their scope to include adjacent security technologies and services like distributed denial-of-service (DDoS) mitigation, API security, and bot mitigation capabilities.
This continuing evolution warrants a new definition and new terminology.

Challenges with a traditional WAF

Organizations with a WAF often claim that it fails to meet initial expectations in terms of effectiveness, ease of management, and impact on protected applications and APIs. Due to web performance issues that often occur from inspecting billions of web and API requests for malicious code, WAFs have often been a source of intraorganizational friction, performance degradation, and obstruction to deployment due to security protocols.

Some of the most significant deployment challenges with traditional WAFs stem from the following:

- Inaccurate detections and high false positives create alert fatigue and additional risk
- WAFs rely on manual review, tuning, and maintenance
- Lack of granular controls lead to heavy-handed deny policies that interrupt end-user experience and business processes
- Out-of-date threat intelligence increases vulnerabilities
- Decreased performance and coverage due to restrictions and inflexibility
- Too limited to protect digital expansion

Traditional WAFs are a powerful security tool. However, they can often leave organizations with operational pains and unmitigated risks that will be addressed in this paper.

Organizations looking to update their WAF technology with a WAAP solution should ensure that the solution delivers both business value and robust security protections. The conversion from WAF to WAAP combines this power of protection with functionality, efficiencies, and ease of use to meet businesses' needs, both for security teams and other teams.

Design principles — WAF to WAAP

As the traditional WAF product focuses on end-user rule creation, any vendor can build a WAF solution and bring it to market with relative ease, as demonstrated by the prevalence of commercial offerings built around the open source Open Worldwide Application Security Project ModSecurity Core Rule Set (OWASP CRS).

However, it is difficult for a provider to design a comprehensive WAAP solution that can:

- Be deployed in-line to protect applications and APIs as new vulnerabilities emerge
- Keep up with modern app development practices
- Provide equally strong layers of DDoS defense, bot mitigation, API protection, and client-side web application protections

As Akamai approached the design of our WAAP solution, we believed it should be more than “good enough.” App & API Protector was created to address security risks while keeping our customer organizations focused on major business objectives. As a blueprint to our design, we believed an ideal WAAP solution should provide:

Effective security
Applications run every aspect of the business. Securing them against malice is the foundational goal of a corporate security team. Security teams are challenged to find a WAAP solution that delivers best-of-breed detections in a WAAP solution. The ideal security tool prioritizes detection efficacy, as it is the most important aspect of a WAAP solution, and has a stellar track record of zero-day, exploit, and Common Vulnerabilities and Exposures (CVE) defense, as well as an impressive availability history.

Accuracy
Security teams need to find the right balance of mitigating risks while enabling the business to move with speed. Ideal solutions will have self-tuning mechanisms that help to reduce false positives while not compromising end-user experience and business processes.

Modern protections

Organizations must continuously (and often manually) update protections to the latest rules to address new vulnerabilities as they are discovered. To do this, they need two key abilities: access to the latest intelligence across attack vectors and skilled security resources that can tailor the defense strategy to meet malleable attacks. An ideal solution will be a leader in the threat intelligence community and provide capabilities that simplify security operations across the estate's protections.

Adaptivity

The threat landscape evolves at a rapid pace. With AI-powered attacks on the horizon, security teams need to be more efficient than ever in their security operations. Ideal WAAP solutions will have a combination of advanced automation, machine learning, and deep global intelligence to deliver updates automatically and provide customized rule modification suggestions that are implemented in a click.

Visibility

Traditional WAF solutions typically provide a never-ending stream of alerts and rely on security practitioners to carefully analyze each alert burning through in-house resources. A more effective WAAP solution provides multi-solution visibility and proactive context around attacks by notifying an organization when, where, and how they occurred to alleviate the resource burden.

Scalability

A solution without enough scale to handle incoming traffic can easily become a bottleneck that increases web latency and has the potential to break under load. An effective WAAP approach seamlessly and automatically scales to match traffic demands and attacks as they vary over time, and provide continuous protection without interruption or reduced performance.

Cooperation

An effective security solution needs to be integrable into the current stack, programmable, simple to use, and frictionless. An ideal solution builds a bridge between security and development teams.

Support

During demanding security events, organizations are often overwhelmed by the skills and resources needed to provide a timely resolution. An ideal solution will have regular managed service options, as well as on-demand service options, that can provide expertise and mitigation for common scenarios including active attacks, services issues, staff turnover, internal skill set gaps, and more.

With these design principles in mind, let’s explore how Akamai approaches building our leading WAAP solution, App & API Protector, starting with the core technology. Our solution combines many security products in one to holistically address challenges in securing applications, defending against volumetric DDoS attacks, protecting APIs across the estate, and controlling bot traffic.

Akamai's approach to WAAP

Moving beyond rulesets

As the market moved from traditional WAF design principles to the modern and effective security solution of WAAP, effective detection and mitigation technology remained the focus.

Akamai first introduced our WAF in 2009 as the world's first edge-based WAF. Security vendors at this time were offering WAFs based on static rulesets as their foundation for detections. Akamai differentiated at that time by building a proprietary rules-based engine called Kona Rule Set, which employed a small number of flexible rules (rather than static rules) in conjunction with an anomaly scoring model to better address accuracy and visibility into attacks.

Then in 2017, Akamai introduced automated attack groups, which eliminated the need for organizations to continually configure and update rules with Akamai-managed protections. Automated attack groups were a revolution, quickly enabled across thousands of active Akamai customer WAF policies to take advantage of this new approach.

Akamai continued to evolve our approach to application security, prioritizing combined application and API protection, including bot defense capabilities, with the launch of App & API Protector in 2021 — this WAAP solution aimed to replace Kona Site Defender WAF for enterprise and growing global businesses. App & API Protector changed the way Akamai approached security operations by modernizing the Kona Rule Set technology into the Adaptive Security Engine.

Modernizing application-layer DDoS defenses beyond rate limiting

When it comes to DDoS, rate limiting is a proven and effective tool. Yet the rise of sophisticated Layer 7 DDoS attacks, multi-vector assaults, and the exploitation of APIs has left traditional DDoS defenses struggling to keep up. Static defenses, which rely on fixed thresholds and predefined signatures, are reactive and prone to false positives, especially as attackers increasingly blend malicious traffic with legitimate requests. This is where Akamai changed the approach to DDoS defense and introduced new innovations such as URL Protection and the Behavioral DDoS Engine.

The Behavioral DDoS Engine is a cutting-edge addition to Akamai App & API Protector, joining the Adaptive Security Engine as one of its core technologies. Together, these engines offer unprecedented protection against modern threats, making Akamai a leader in WAAP. This dual-engine approach sets Akamai apart by delivering automated updates, self-tuning capabilities, and context-aware detection for a hands-off experience.

Single solution for comprehensive protection

Today, change continues to redefine application security with modern development practices via serverless edge computing, microservices-based architectures, single-page applications, and SaaS/IaaS/PaaS/FaaS approaches being used that shape application security.

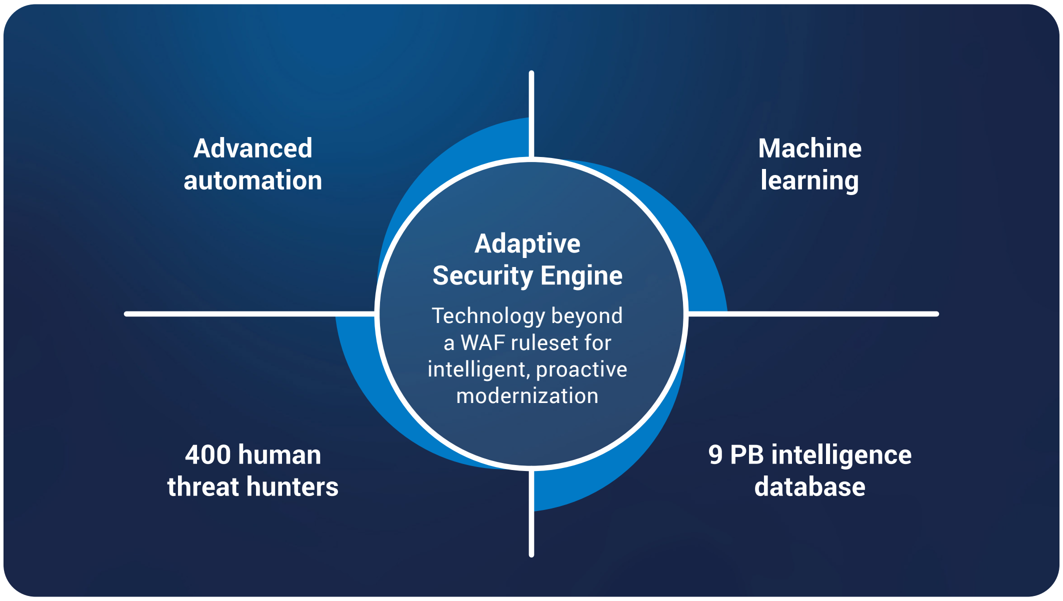
To protect modern applications and APIs in complex IT environments, Akamai re-architected our application security technology with a more adaptive, flexible, and holistic approach. As Akamai's WAAP solution migrated from Web Application Protector and Kona Site Defender to App & API Protector, more security capabilities and featured toolsets were incorporated.

App & API Protector now provides many additional security enhancements, all of which are visible and controlled via a single interface. Akamai's WAAP solution combines:

1. An Adaptive Security Engine
2. Application security with granular controls
3. DDoS defense, including advanced Layer 7 DDoS protection
4. API protection, including discovery and PII protection features
5. Bot visibility and mitigation capabilities
6. A platform for global scale, threat intelligence, and resiliency

The Adaptive Security Engine

The Adaptive Security Engine provides next-generation protection at the intersection of machine learning (ML), real-time security intelligence, cybersecurity experts, and advanced automation. As Akamai's core technology for detection and defense, the Adaptive Security Engine enables a hands-off approach to protect entire web applications and API estates. It also adds to Akamai's advancements from WAF to WAAP, which incorporate correlating security solutions including bot manager, DDoS protection, DevOps integrations, and more.


Advanced automation
Machine learning
Adaptive Security Engine
Technology beyond a WAF ruleset for intelligent, proactive modernization
400 human threat hunters
9 PB intelligence database

The Adaptive Security Engine 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. It uses the same platform insight and intelligence to reduce false positives via tuning recommendations. This self-tuning feature offers ease of use by security and development teams by delivering adaptive threat protections as proactive updates.

Adaptive threat detection

The engine employs a multidimensional threat scoring model that combines platform intelligence with data/metadata from each request. This data is actioned with decision-making logic to accurately identify true attacks.

Adaptive detections are especially effective in identifying highly targeted, evasive, and stealthy attacks since sophisticated attackers invest more time and effort in their approach. As attackers scan for vulnerabilities and misconfigurations, the Adaptive Security Engine collects and correlates evidence about their tactics to make attackers' historical fingerprints more identifiable.

In addition to the actual payload and its location within the request, other examples of attack dimensions it evaluates for each client include:

- A history of reconnaissance and/or attacks (e.g., frequency, magnitude, severity)
- Any sign of malicious automation and attack tooling
- Correlation to known sources of attack traffic

Moreover, the Adaptive Security Engine is enhanced with two proprietary technologies: Smart Detect, which tokenizes the input into a fingerprint for highly accurate detection, and Smart Sniff, which detects the right content type of the request body to prevent content manipulation and bypass. Akamai threat researchers leverage Akamai's expansive infrastructure and systems to passively run new detections across all production traffic and then analyze those results using ML models.

Automatic updates

Many organizations today have insufficient resources or security expertise to continuously track developing threats, update configurations, and retest against their web traffic to optimize policies. In response, Akamai continuously updates the Adaptive Security Engine using an AI/ML automatic testing framework to account for changing threats while maintaining high accuracy. These updates have often protected against zero-day attacks before they were announced.

Testing framework to ensure accuracy

Testing a WAAP solution relies on a simple premise: Test different attack vectors and stop web attacks. However, the following factors need to be considered:

- Real-world environments are more complex than test environments and often lead to false positives and false negatives.
- Designing a testing framework with accuracy in mind requires additional verification — not just attack detection, but doing so without inadvertently triggering false positives or false negatives.
- Testing requires the use of real web traffic — both legitimate and attack traffic.

Adaptive Security Engine updates consist of multiple stages to ensure legitimate traffic is not adversely impacted:

- All detections are lab tested using synthetic traffic to ensure they properly catch attacks while not introducing false positives.
- Updates are then tested on live production traffic to ensure the sample is valid for current platform traffic. This process involves running the update in shadow mode on real customer traffic. Running in shadow mode ensures no impact to customer traffic while still running test detection accuracy.
- Once an update has passed stage two, ML identifies patterns or triggers that human analysis may have missed, after which the Threat Research Team manually reviews results.
- Only when these checks are passed at each phase can a change move to the next phase and be deployed to a larger segment of the network. After 100% deployment, self-tuning capabilities will eliminate any remaining false positives particular to customers’ traffic patterns.

Automatic self-tuning

Automatic self-tuning alleviates the burden of manual tuning, which can lead to outdated policies and human error, for a near-hands-off experience. The Adaptive Security Engine applies ML, statistical models, and heuristics across all triggers for each security policy to accurately differentiate between real attacks and end-user traffic misidentified as attacks. It is not a generic platform-wide check that is applied only during onboarding, but rather a continuous tuning process performed 24/7/365 with no end-user configuration or intervention.

Self-tuning is frictionless and simple. Security administrators can easily review and accept recommendations with one click via the user interface, or they can automate using AppSec APIs, command-line interface (CLI), or Terraform. For greater transparency, a pre-filtered link to Web Security Analytics shows all requests deemed as false positives with a rationale provided for each tuning recommendation.

Configuration and automation flexibility

When a WAAP solution vendor moves past the traditional ruleset technology, configuration and automation become more flexible. The Adaptive Security Engine grants the ability to:

- Have different types of WAF updates (auto vs. manual) for different applications and their associated risk appetite
- Control action per attack group and contributing rule necessary for customization if application/traffic behavior is not standard
- Set up simple and complex conditions for different request characteristics such as IP, geo, header, payload, etc.
- Proactively mitigate threat sources that have been detected carrying out suspicious WAF attack/scanning for your own apps, with Penalty Box
- Modify debug header
- Modify request payload inspection size or attack payload logging settings
- Run simulations of change in detection logic to confidently push these changes on production

Verify in the real world

Evaluation mode provides Akamai customers with flexibility and granularity in configuring specific Adaptive Security Engine versions and testing updates or new rules/policies. Customers can see new updates or changes before choosing to enable as appropriate or necessary for their specific web application environment. For effective security modernization, Akamai believes that testing on real-time traffic improves security outcomes over testing on past traffic. Evaluation mode is similar to applying a shadow rule where you can see the real-time results as if the policy were enforced — yet with no impact to current end users. Organizations can opt for this manual/evaluation mode of operation to minimize unexpected impact on false positives and false negatives.

Integrating modernized protections

Security and DevOps teams can also operationalize security by integrating calls to Akamai APIs using the CLI, Akamai Terraform, or scripts in their CI/CD automation pipeline. Configuration and automation flexibility ensure that powerful security never hinders development velocity. These integrations can:

- Enable rapid onboard applications
- Provide uniform management of security policies across large application portfolios
- Centralize security enforcement across hybrid and multicloud infrastructures
- Improve collaboration between DevOps and security teams in a GitOps workflow for optimal coverage

Additionally, security information and event management (SIEM) allows you to collect security events that take place on the Akamai platform. In turn, our SIEM Integration solution provides a way to deliver SIEM events to on-premises and cloud-based SIEM analytic tools such as Splunk and QRadar so you can incorporate Akamai security events into your overall eventing and security infrastructure in four basic steps.

You can protect and control your data feed with:

- **Event filtering**
  Use security configuration and security policy to help you focus on real threats.
- **Data retention**
  The collector stores data for 12 hours so you can capture missed events.
- **SIEM overload protection**
  In your SIEM connector, you can define the maximum number of security events fetched in each request. This helps you avoid overloading the SIEM application.
- **Fetch interval**
  You can define how often the SIEM connectors make a call to the SIEM API to fetch security event data.

Application security and DDoS defense

Application security is a crucial aspect of modern cybersecurity, ensuring that applications remain resilient against a wide range of threats and vulnerabilities. Its importance lies in several key areas. Data integrity and confidentiality are paramount, as application security ensures that sensitive data is protected from unauthorized access and tampering. It also plays a vital role in business continuity by protecting applications from disruptions caused by security incidents, thereby ensuring consistent service availability. Additionally, application security is essential for reputation management, preventing breaches that can damage an organization's reputation and erode customer trust. Lastly, it helps organizations comply with regulatory requirements, thereby avoiding legal and financial penalties.

Functionally, a WAAP solution filters and monitors HTTP traffic between web applications and the internet. This protects against common web-based attacks like XSS, SQL injection, and DDoS.

App & API Protector is recognized for its market-leading DDoS protection, designed to counter volumetric attacks aimed at overwhelming resources. The solution combats DDoS in the following ways:

- **Edge-based DDoS mitigation**
  By leveraging Akamai's globally distributed edge platform, App & API Protector can instantly drop DDoS attacks before they reach the application origin. This edge-first approach ensures minimal latency and maximal protection without affecting the performance of the application.

- **Rate limiting**
  App & API Protector includes adaptive rate limiting to defend against distributed application-layer DDoS attacks. These controls can be configured to limit the rate of incoming requests based on various criteria including but not limited to IP, geo, IP reputation controls, various HTTP headers, and match conditions.

- **URL Protection with intelligent load shedding**
  Takes a different approach to rate limiting. With URL Protection, you can protect your origin from excessive requests based on the acceptable request rate (maximum RPS) depending on origin capacity. It is specifically designed to protect compute-heavy URLs, API endpoints, etc. from highly distributed application-layer DDoS attacks.

- **Behavioral DDoS Engine**
  New to App & API Protector, the Behavioral DDoS Engine is a powerful tool to a defense-in-depth strategy. It introduces a hands-off approach of managing and mitigating DDoS events by using ML in establishing traffic baselines and identifying anomalies against the norms. The engine works by understanding the changing traffic patterns and allows users to define how the system reacts to different anomalies without setting explicit thresholds, reducing the operational burden of managing and tuning the system.

- **Automatic updates and adaptive self-tuning**
  Using Akamai's two-engine strategy, the Adaptive Security Engine and the Behavioral DDoS Engine, App & API Protector continuously adapts to new threats through automatic updates and ML-driven self-tuning to reduce operational burden.

Behavioral DDoS Engine: How it works

At the heart of the Behavioral DDoS Engine is an advanced ML model that continuously monitors real-time traffic, establishing baselines for normal behavior and instantly detecting deviations that indicate an attack. By analyzing traffic patterns across multiple dynamic dimensions — such as country source, TLS patterns, IP, and TLS fingerprints — this engine can swiftly identify anomalies and take action.

Key components of the Behavioral DDoS Engine include:

- **Real-time behavioral monitoring**
  The engine continuously analyzes traffic to establish baselines of normal activity and instantly detects deviations that signal potential DDoS attacks.

- **Machine learning for precision**
  Advanced ML models power the engine's ability to identify subtle anomalies in traffic patterns, ensuring accurate mitigation without blocking legitimate users.

- **Proactive mitigation**
  By leveraging Akamai's global network insights (1,056 TB of traffic per day), the engine predicts and neutralizes attacks, often before they can impact businesses.

- **Multidimensional analysis**
  Traffic is evaluated across multiple dimensions, including IP, country, and TLS patterns, providing robust protection tailored to each application's needs

Advanced architecture for superior defense
The Behavioral DDoS Engine operates through a sophisticated architecture that includes several critical components:

- **Detection engine**
  Uses dynamic dimensions and historical attack data to identify DDoS attacks in real time.

- **Mitigation engine**
  Automatically counters attacks using intelligence from the baseline generator and threat signals, reducing operational overhead for security teams.

- **Noise/false positive reduction**
  ML models filter out irrelevant data, ensuring clean traffic is used for analysis and mitigation.

- **Baseline generator**
  Continuously refines traffic profiles by processing cleaned data over a two-week period, allowing the engine to stay updated with the latest attack strategies.

- **Baseline validator**
  Aided by AI, this crucial component evaluates hundreds of DDoS attacks each month to fine-tune the solution.

This automated framework ensures that security teams can rely on the engine to dynamically adjust defenses without manual intervention. The solution detects abnormal traffic activity, such as bot-generated traffic or DDoS attempts, and filters it out to protect applications effectively.

Application security accuracy

An application security solution (WAF or WAAP) that is not accurate requires more internal resources to manage the increased number of daily alerts. Inaccuracy can deliver a large number of false positives (where a request is flagged as malicious when it isn't) and false negatives (where a request is flagged as not malicious when it is), wasting valuable security skill sets and time on the research and analysis of these types of alerts.

Organizations often experience the challenge of alert fatigue but remain without a solution due to too broad of controls or capabilities that over- or under-correct. This often leads the organization to pull their WAF offline — or worse, disregard the alerts and version updates. While this alleviates many organizational concerns about accidentally blocking legitimate users, it also protects against fewer web and API attacks. Many organizations also lack the granularity of controls to balance access for legitimate traffic and blocking malicious traffic with precision.

The benefit of an effective WAAP solution is that it lowers both false positives and false negatives to increase precision and minimize impact on legitimate users with a comprehensive set of WAAP controls and capabilities.

Understanding accuracy

Accuracy measures the ability of a WAF or WAAP to simultaneously stop attacks while not inadvertently blocking legitimate users. It considers four variables:

- **True positives (TP):** Real attacks that are properly identified as malicious
- **False positives (FP):** Legitimate requests that are improperly identified as malicious
- **True negatives (TN):** Legitimate requests that are passed through to the application
- **False negatives (FN):** Real attacks that are improperly passed to the application

Client Reputation scores

Client Reputation uses a sophisticated risk-analysis engine to compute a set of "risk scores" for each IP address that tries to access your site. It analyzes the incoming IP addresses and uses various factors such as attacker persistency, number of targeted applications, severity of the attack, magnitude, industry, and previous attacks targeting a customer's applications to determine a score that specifies the likelihood of this IP address engaging in a web attack, including:

- **DOSATCK**
  This uses botnets to launch denial-of-service (DoS) attacks. The goal of a DoS attack is to flood a site with so many bogus requests that the site becomes unbearably slow, or even crashes. In a distributed denial-of-service (DDoS) attack, these requests come from thousands of locations (typically malware-infected computers or phones), making it impossible to stop the attack simply by blocking a given IP address.

- **SCANTL**
  Scanning tools can identify potential security risks such as SQL injection, cross-site request forgery (CSRF), invalid redirects, and other vulnerabilities. Running a web scanning tool against your own site is a good idea. Having a malefactor run a scanning tool against your website isn't quite as good.

- **WEBATCK**
  Uses techniques such as SQL injection, remote file inclusion, or cross-site scripting to do things like install malware or steal user data. A hacker might be able to retrieve all your user data, including passwords, credit card numbers, Social Security numbers, and any other information you might have stored in the user database.

- **WEBSCRP**
  Uses automated tools to download a copy of a web page and then "scrape" (i.e., copy) all the content on that page. The content may be repurposed for illegal or unethical uses.

With Client Reputation, you can shield your organization proactively from suspicious threat sources based on the cumulative threat intelligence from Akamai Connected Cloud.

Malware protection

Threat actors use malware as a common attack tactic. For comprehensive protection of applications, Akamai has a solution to protect against malware. Organizations of all sizes allow file uploads for efficiencies both inside and out, including these common uses:

- Resumes for job applications
- Employment agreements, onboarding, E-Verify, direct deposit setup, and more
- Applications, including loans, account setup, and credit requests
- Insurance or repair estimates for auto, home, and more
- Medical records for insurance or patient account setup
- Customer product or experience reviews that include images

Malware protection within app and API security detects and isolates malware threats at the edge before they reach their target corporate system. Organizations can protect time, budget, and productivity, as well as internal and customer data, with the benefits of malware protection for apps and APIs:

- **Detect and block malware at the edge**
  Avoid the risks of scanning on servers, where the malware could have already spread by the time it's scanned.
- **Avoid complexity and free up time**
  Scan files only once, rather than setting up protection in each system individually, as with ICAP and agent-based scanners.
- **Position security posture for growth**
  By choosing a preventative and layered approach, organizations can scale their protection as business grows, providing extra protection at the edge and the option to scan again at origin.
- **Provide consistency to your applications**
  Businesses do not have to configure or change application code. Malware protection is hosted completely on Akamai Connected Cloud.

Application security analytics

Included in App & API Protector is Akamai's most-loved (and most-used) product: Web Security Analytics. This Akamai WAAP solution allows you to capture the security events that take place against your web application and APIs on the Akamai platform and visualize them in the provided security analytics tools.

Web Security Analytics is a vital component of modern cybersecurity, offering comprehensive insights into web traffic and potential threats. By analyzing a vast array of data points, including traffic patterns, user behavior, and security events, it provides detailed visibility into the security posture of web applications. This proactive approach enables organizations to detect and respond to threats more effectively, mitigating risks before they can cause significant damage. Web Security Analytics not only helps in identifying malicious activities, such as bot attacks, SQL injections, and cross-site scripting, but also aids in understanding and addressing vulnerabilities within the web applications. Moreover, it supports compliance efforts by generating reports that demonstrate adherence to security policies and regulatory requirements.

API Discovery and Profiling

APIs allow organizations to create powerful web and mobile experiences, often by exposing back-end data and logic to develop new and innovative offerings. APIs also expand the attack surface. Organizations need an understanding of which API endpoints are in their environment, the API's functions, and their traffic profiles. Akama's API Discovery and Profiling capability does just that and more, automatically and continuously.

The API Discovery feature alerts security teams to new, often unprotected, apps and APIs that are connected by different lines of business in an organization. This automated detection technology is a new feature of Akamai's WAAP solution to keep development teams, line-of-business leaders, and security teams aligned.

The Adaptive Security Engine automatically discovers APIs every 24 hours based on a scoring mechanism that takes into account response content type, path characteristics, and traffic patterns. The discovery data includes information on the observed API specification with details such as:

- Hostname
- Basepath
- Resource path
- Parameters and their data type
- Methods
- Format of the API

Base and resource paths are determined based on an algorithm that takes into account path depth, children count, and siblings from the observed traffic on a specific hostname with API traffic. Within the resource path, if a parameter is observed for a specific method, it is marked, and the data type of that parameter is identified.

The traffic profile for the API endpoints contains information that gives insight into the API's purpose and current threat level. Some of the data points included are:

- Total requests since the API was first discovered, both in the past 24 hours and trending over time
- Date the API was first discovered and last seen
- Number of requests across different methods like GET, PUT, POST, DELETE, and OPTIONS
- Number of requests generating 2xx, 3xx, 4xx, and 5xx responses
- End-client identification based on user agent
- Response errors such as the percentage of traffic resulting in client-side and server-side errors
- Hits from known threat actors — including the percentage of total traffic coming from known malicious actors to the Akamai platform — split by web attackers, web scanners, scrapers, and DoS attackers

Protecting APIs can be a significant hurdle without visibility. How does an organization protect what it can't see? With Akamai, businesses can automatically and continuously discover and profile APIs, including their endpoints, definitions, and resource and traffic characteristics. Once APIs are identified, Akamai provides broad protection to deal with DoS, malicious injection, credential abuse attacks, and API specification violations. Akamai's cloud- and origin-agnostic approach allows for easy API discovery across an entire application estate without any additional configuration required by the end user. This visibility enables developers, application owners, and security teams to stay ahead of new, unknown, or changing APIs — and easily register them for protection.

Bot visibility and mitigation

With bots contributing more than half of website traffic, it can be difficult to know which bots are helping your organization achieve goals and which have the intent to harm. Good bots create efficiencies in the organization by automating evaluations, conversations, or recommendations. Bad bots can clog up traffic paths and impact customer and operational experience, affecting revenue. Within App & API Protector, Bot visibility and mitigation gives powerful detections to see good bots and let them through, while blocking bad bots. This allows organizations to:

- **See bots and understand their impact**
  Visibility into bot traffic is critical for modern digital businesses, given the pervasive use of bots for operations like searching, checking site performance, and interacting with business partners.

- **Improve operational control**
  Blocking bad bots allows enhanced efficiency, reduces business and financial risks, and better controls IT spend.

- **Make better, data-driven decisions**
  Detailed analytics and reporting help to make creative and effective choices about customer journeys, security posture, risk tolerance, and IT operations.

Bot visibility and mitigation intrinsic to App & API Protector

App & API Protector offers bot detections and controls for bot traffic that may adversely impact the performance and security of web properties. It provides early visibility to proactively monitor for bot-related anomalies and threats that develop over time.

Using Akamai's bot solution delivered in App & API Protector:

- Access over 1,700+ defined bots known to Akamai
- Gain real-time bot traffic visibility
- Create custom bot definitions
- Allow good and deny bad bots
- See bot visibility and trend reporting

For sites with advanced bot problems, Akamai offers Bot Manager, which includes advanced bot protections for increased ecommerce and digital security. Bot Manager provides more nuanced actions for persistent, adversarial bots like those used for attacks such as:

- Credential stuffing
- Inventory hoarding
- Content and price scraping
- Business logic abuse

Key bot capabilities

Akamai recognizes the evolving needs for bot management via WAAP, and elevated our bot visibility and mitigation tools to include newly incorporated capabilities such as:

- **Browser impersonation detection**
  This customer favorite of Akamai Bot Manager uses dynamic scoring models and ML to discern and counteract in-browser bot activities, and is included in App & API Protector.
- **Conditional response actions**
  Customers now have an improved understanding of in-browser bot activities and can respond with conditional actions to apply different response strategies against malicious bots.
- **Challenge actions**
  Address bots with a range of different challenge actions, including interstitial challenges that, when unsolved, provide the ability to block access to the content.

More than a WAF: Benefits from the Akamai solution

Akamai's approach to WAAP resulted in the solution App & API Protector. However, there is more than a single product that benefits our WAAP customers. Built on the most distributed global platform and powered by hundreds of human threat experts, Akamai Connected Cloud delivers performance, availability, intelligence, expertise, and effective security outcomes.

Threat intelligence and detection

Having a robust and in-house threat intelligence capability improves a WAAP vendor's ability to respond to developing threats. However, the quality, timeliness, and actionability of the intelligence provided will determine the amount of impact on application security effectiveness. Akamai continuously analyzes the data available through Akamai Connected Cloud to identify current trends in the threat landscape, new attack vectors as they are first seen, and currently active attackers. Akamai then incorporates that intelligence into our WAAP solution in multiple ways.

The Akamai Adaptive Security Engine, featured earlier in this paper, combines two tiers of deep threat intelligence to create a powerful and proprietary engine to manage the latest protections automatically for our customers. In addition to ML and automated rule adoption, the Adaptive Security Engine features threat intelligence from Akamai's global platform and a large team of expert threat researchers.

Akamai platform intelligence

Having one of the largest global platforms provides Akamai with the mechanism to analyze attack traffic on a global scale against every Akamai customer in a timely manner. Our intelligence database includes an average of 1,056 TB of attack data every day. It leverages Akamai's visibility into web traffic to thousands of the largest, most heavily trafficked, and most frequently attacked online businesses to acquire relevant and high-quality data for analysis by Akamai's Threat Research Team:

- **WAAP triggers**
  Ingests data directly from Akamai's global WAAP deployments, capturing actual attack events targeting every Akamai security customer.

- **CDN logs**
  Incorporates offline analysis performed on event logs from every Akamai customer, including those that have not deployed their WAAP solution.

Akamai's intelligence database houses one of the largest datasets in the world (9 PB). For organizations prioritizing the security of their businesses and customers, Akamai's threat intelligence leads WAAP solution providers.

Threat research and incident response

Threat research and incident response organizations provide human intelligence and analysis to complement and broaden the attack coverage of a WAAP solution. Akamai employs multiple teams with different charters to support our WAAP customers, as well as identify new attack vectors that may require additional protections.

Threat research

The Akamai Threat Research Team performs regular analysis of web attack trends across the entire Akamai customer base, as well as custom analysis for individual customers as required. The team also designs and implements heuristics to query for actionable intelligence to support the creation and updates to the core WAF rule logic and Client Reputation.

Incident response

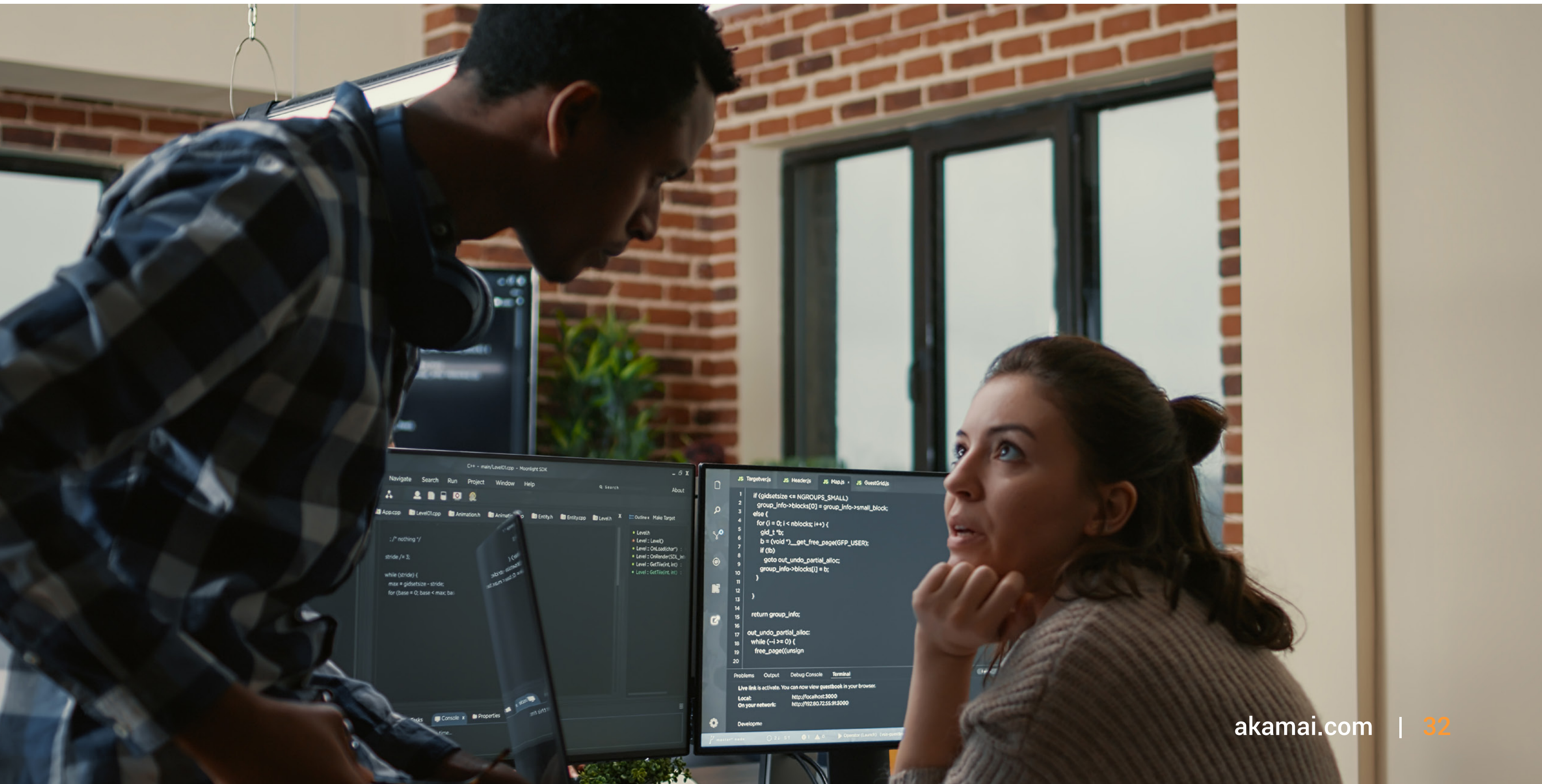
Akamai operates two incident response teams — the Computer Security Incident Response Team (CSIRT) and Security Intelligence Response Team (SIRT) — to work with Akamai's global security operations center (SOC) and provide analysis and incident response for individual customers when they experience an attack. In addition, CSIRT monitors frequently attacked Akamai customers, representing a broad range of industries as a leading indicator of new attack vectors or trends.

Rapid threat detection

Our new capabilities enable swift deployment of protections against emerging threats and high-profile CVEs. Automatic updates and the option for "Akamai-managed" actions mean that you can manage your defenses with agility.

CVE protection

The Akamai Threat Research Team continues to monitor Common Vulnerabilities and Exposures, and ensures that the WAAP solution is updated to protect customer applications and provide necessary confirmation through the Akamai CVE lookup tool. This tool helps by providing detailed information on CVEs, including threat levels and insights into Akamai's current protections. Akamai's CVE protection catalog provides you visibility so you can prioritize security efforts in alignment with Akamai's protections, and allows you to search the CVE database to determine Akamai's active protective measures against a vulnerability, as well as assess threat level and access CVE details.



Globally distributed edge platform

Reliability and resiliency

Premium WAAP solutions are built on extensive, powerful networks that do not cap customers' good traffic in even the largest cyberattacks. The proven quality, capacity, and execution ability of a WAAP provider's global platform should be equally important to the features of the solution. When a WAAP provider fails to deliver good traffic during an active attack, customers should evaluate whether they invested in a solution or just a tool.

Akamai is devoted to delivering industry-leading performance and protection to our customers. This mission is possible only by building services on the strongest foundation: Akamai Connected Cloud. Akamai has built the world's most distributed cloud platform made up of 4,200+ edge PoPs in 130+ countries.

Akamai's customers include all top 10 brokerages, all top 10 banks, all top 10 video streaming services, and all top 10 gaming companies. Our customer base ranges from most of the top automotive companies, healthcare providers, retail, and telecommunications carriers to a significant number of government agencies and the armed forces.

These customers place their trust in Akamai's abilities to power and protect them from the 40 billion bots per day, 780 million app attacks per day, and 1,889 DDoS attacks per quarter that threaten to take down their networks. Akamai successfully delivers security because the threat intelligence gained by one customer benefits and applies protections to every customer. The scale of Akamai's global platform delivers both the quantity and quality of data needed to secure organizations moving into the AI era.

Visibility at Scale Powers Vast Intelligence

Akamai is trusted to protect many of the globe's largest brands across industries. The threat intelligence gained by a single customer applies protections to all.

Akamai Customers:
All top 10 video streaming services
All top 10 video game companies
All top 10 banks
All top 10 brokerages
9 of the top 10 software companies
9 of the top 10 telecommunications carriers
9 of the top 10 healthcare providers
9 of the top 10 retail companies
8 of the top 10 automotive companies
7 of the top 10 healthcare payers
7 of the top 10 fintech companies
7 of the top 10 pharma companies
All 6 U.S. military branches
14 of 15 U.S. federal civilian cabinet agencies

over
780M app attacks
per day

over
40B bots
per day

83B
web app attacks
per quarter

average data
1,056 TB
per day analyzed

1,899
DDoS attacks
per quarter

Global scale

For a WAF, the issue of scale revolves around both its ability to inspect the required volume of web traffic, initially and as it increases over time, and the number of WAF rules required to evaluate that traffic against. Traditional hardware-based WAF solutions often suffer from poor scale because they are limited to the CPU and memory resources available within the appliance and may have to compete with other solutions on the same appliance.

Deploying an integrated WAAP solution across Akamai's cloud platform eliminates the issue of scale by leveraging Akamai's distributed server resources to inspect incoming web traffic. Users and attackers connect to protected websites through the closest Akamai server, which then inspects traffic for attacks and blocks any detected malicious requests. This allows Akamai's WAAP solution to scale seamlessly with any increase in the amount of web application traffic — both sudden spikes in traffic and long-term growth — as well as with new user locations around the world.

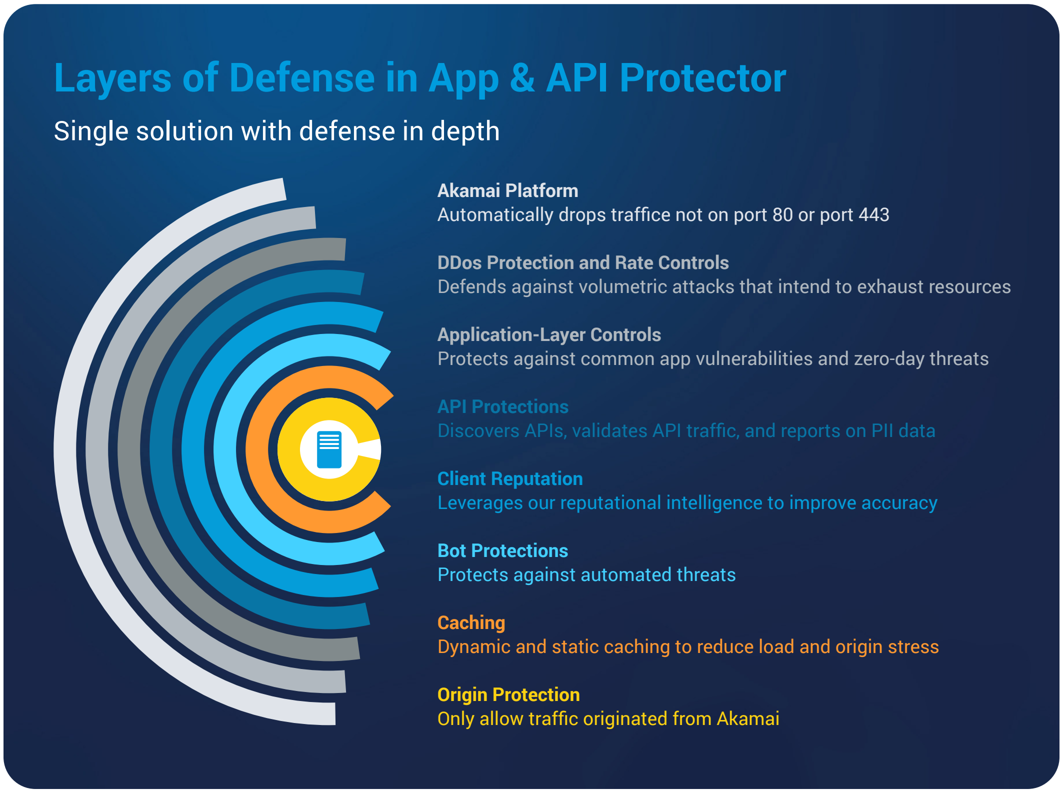
Performance

Poor performance can hinder the deployment of a security solution — especially a WAAP solution deployed in-line in front of an application. Reducing the performance of websites that are critical to business can lead to decreased productivity, poor user experience, slower time to market, and reduced revenue.

The global scale of Akamai's cloud platform allows the WAAP to protect web applications without reducing performance. The globally distributed WAAP inspects HTTP traffic as it first comes onto the platform, distributing the CPU and memory resources required to inspect that traffic across all the servers on the platform. This removes the issue of performance as a source of intraorganizational friction and an obstruction to deployment.

Edge platform powers protection

Akamai’s cloud-agnostic web application security solutions work seamlessly across the platform to defend against a wide range of application and API-based attacks. The image below illustrates the full stack of Akamai’s layered security mechanisms and controls used to keep threats far away from the origin while improving performance and access for legitimate users.



Layers of Defense in App & API Protector

Single solution with defense in depth

Akamai Platform
Automatically drops traffice not on port 80 or port 443

DDos Protection and Rate Controls
Defends against volumetric attacks that intend to exhaust resources

Application-Layer Controls
Protects against common app vulnerabilities and zero-day threats

API Protections
Discovers APIs, validates API traffic, and reports on PII data

Client Reputation
Leverages our reputational intelligence to improve accuracy

Bot Protections
Protects against automated threats

Caching
Dynamic and static caching to reduce load and origin stress

Origin Protection
Only allow traffic originated from Akamai

Akamai App & API Protector includes a broad range of security mechanisms and controls automatically built in (depicted in blue) for a holistic defense straight out of the box, while additional Akamai products and services are added for complete Layer 7 protection

Managed attack support

In addition to ongoing WAAP management, Akamai also provides customers with managed attack support — 24/7 monitoring of protected websites and a managed response to any detected attacks.

Managed attack support utilizes staff in Akamai's global SOC to respond to security incidents as they occur by:

- Responding to WAAP alerts and customer requests and performing further investigation of issues
- Determining an appropriate attack signature and deploying additional mitigation measures
- Working with customer application teams to measure the effectiveness and accuracy of deployed mitigations, adjusting mitigations as necessary
- Reviewing overall response with customer application teams after the incident
- Providing attack alert buttons in the interface to initiate an emergency support request

Security Operations Command Center (SOCC)

Akamai's SOCC has helped mitigate many of the largest attacks worldwide for over 10 years, protecting customers from an ever-evolving global threat landscape.

Monitoring and mitigating a malicious attack requires four features:

- Global visibility
- Proactive monitoring and alerting
- Agile attack mitigation
- Continuous advisory service by an experienced security team

The Akamai SOCC delivers these capabilities by operating the largest security infrastructure in the world. All network traffic runs across our unified security platform, which gathers intelligence in real time. For example, Akamai gathered security trends such as a recent large increase in SQL injection attacks.

All this helps Akamai's security team mitigate customer threats rapidly with maximum effectiveness and minimum impact.

Conclusion

In addition to protecting against network and application-layer DDoS, new forms of automated bots and targeted attacks via APIs and client-side components mean organizations must protect all their web applications, API endpoints, browsers, and infrastructure with a holistic defense-in-depth security approach. Security leaders and practitioners need web application security that quickly identifies and mitigates threats from multiple attack vectors and extends traditional protections beyond the firewall to adjacent security technologies for the best security defense.

Akamai's approach to WAAP is to offer a solution set that is unmatched in its breadth and effectiveness because it provides all of the security technologies needed for a modern security posture. We believe that the leading security solution shouldn't be for just the globe's largest or most popular brands. Our portfolio for app and API protections makes effective web app security available to any security-first organization through a tiered portfolio.

With a security solution that continuously evolves and adapts, actioning off deep and wide attack intelligence, Akamai partners with global businesses to modernize and continually improve security outcomes. We look to empower your organization's security teams with the intelligence, visibility, automation, and guidance to drive internal initiatives while keeping adversaries out of your corporate systems. That is why we are trusted to protect the most demanding brands that power life online.

Akamai Security protects the applications that drive your business at every point of interaction, without compromising performance or customer experience. By leveraging the scale of our global platform and its visibility to threats, we partner with you to prevent, detect, and mitigate threats, so you can build brand trust and deliver on your vision. 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 and LinkedIn. Published 02/25.