



SOLUTION BRIEF

# WafCharm: the force multiplier for AWS WAF operation

Automatically configure and optimize AWS WAF for greater protection

## Add another layer of defense

Keeping your applications and infrastructure protected from bad internet protocols (IPs), data theft, and malicious bots is critical for organizations hosting assets on Amazon Web Services (AWS). For organizations utilizing the Amazon CloudFront content delivery network (CDN) to deliver apps, AWS Shield is built in and provides distributed denial of service (DDoS) protection.

AWS WAF provides defense for your web applications, application programming interfaces (APIs), and infrastructure. AWS WAF enables you to create security rules that provide more control over the traffic reaching your applications. Users need to configure and build these rules within AWS WAF themselves or with the expertise of a security engineer and continuously manage those rules. This enables custom configuration for full transparency. For customers who have limited resources or do not have in-house expertise, the process can be time consuming and costly.

WafCharm is an automated managed service that sits on top of your AWS WAF to simplify and strengthen your firewall protection. WafCharm not only responds to new vulnerabilities quickly but also helps reduce false positives by configuring WAF rules that are unique to your application.

## Add protection and ease

WafCharm is effective both for users who do not have the personnel or resources to set up or maintain AWS WAF security rules and advanced users looking to add enhanced protection to the existing WAF rules they have in place. WafCharm technology makes security implementation simple. Customers simply create an AWS WAF maintenance role and Amazon Simple Storage Service (Amazon S3) bucket and let WafCharm handle the rest. WafCharm also provides step-by-step educational materials to secure your most vulnerable data.

WafCharm's rules are integrated in AWS WAF with full transparency so there's no need to add a separate platform. Cyneural, WafCharm's artificial intelligence (AI)-based attack detection, analyzes web traffic patterns to distinguish desired users from malicious ones. Then Waf Rule Automated Operation (WRAO), WafCharm's AI-based automatic rule operation, automatically optimizes security and updates rules based on its findings.

WafCharm's continuous monitoring and automatic rule updates helps keep your AWS environment more secure in the ever-shifting landscape of online threats. Your traffic is analyzed constantly to tailor protection specifically to your environment. WafCharm is customizable and learns from rules your team already has in place without disrupting or altering the existing rules or system, allowing IT and security teams to focus on other strategic initiatives.

In collaboration with



## Key benefits of

# WafCharm

- Provides additional layer of protection for advanced web application firewall (WAF) users
- Simplifies the security, deployment, and management of AWS WAF
- Automatically configures, curates, and updates AWS WAF rules
- Utilizes AI to analyze traffic to continuously update rules
- Greatly reduces false positives, keeping site traffic flowing
- Supported by Cyber Security Cloud security experts
- Built on AWS which allows easy integration



## Add security expertise

WafCharm collects threat data in two ways: with advanced threat intelligence and a team of security experts. After collecting the threat information, the security expert creates, verifies, and updates the WAF rules, so customers don't have to. Cyber Security Cloud's security experts provide support through customer service and security advisory recommendations, enabling customers with limited resources or knowledge to maintain the highest levels of security without hiring additional staff.

## Add the scale and strength of AWS

WafCharm is built on AWS and fully integrated into your AWS environment. WafCharm utilizes Amazon Elastic Cloud Compute (Amazon EC2) to respond to new vulnerabilities quickly.

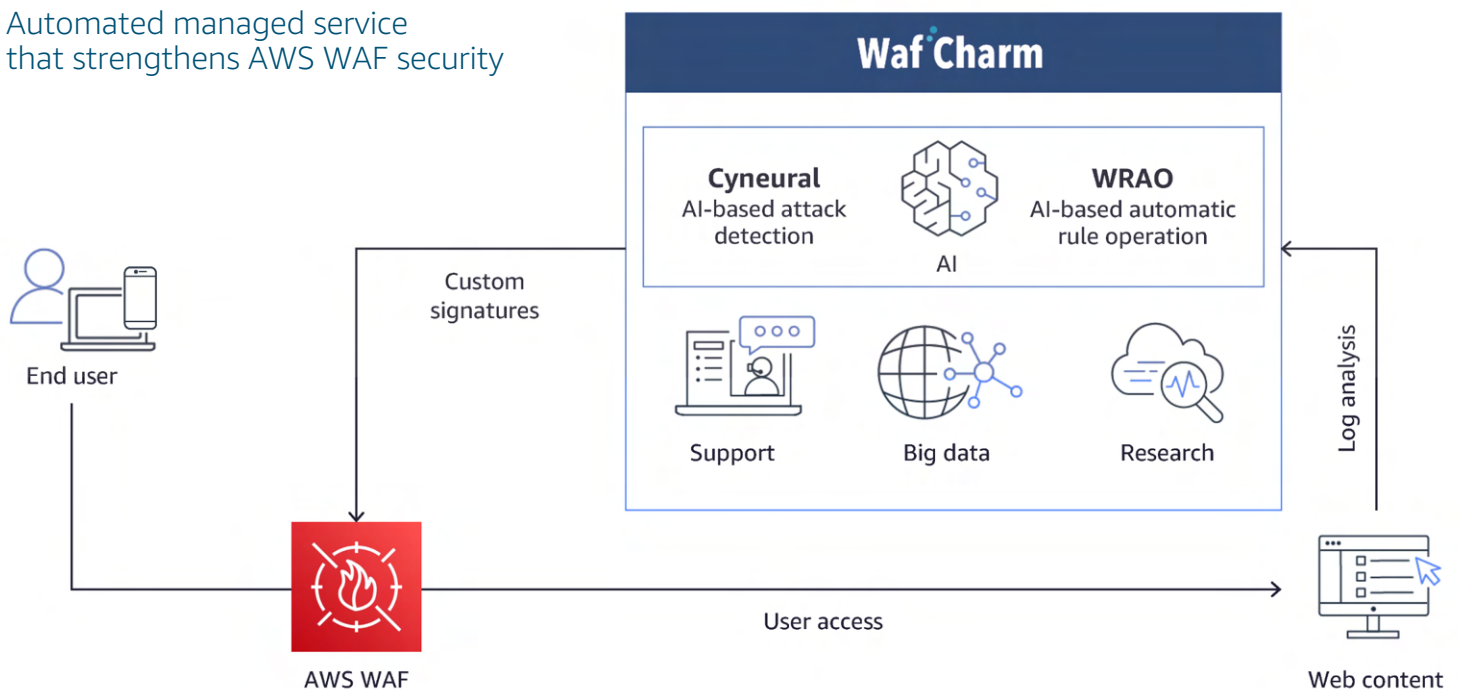
WafCharm uses your AWS dashboard for streamlined visibility. Monthly reports are generated at no additional cost. Logs and streams are analyzed to study the past, protect the present, and predict future traffic. This is particularly helpful for organizations operating within compliance-heavy industries such as financial services, healthcare, and government.

Paired with the AWS pay-as-you-go consumption model, WafCharm's competitive pricing can help offset operational costs.

AWS WAF is supported by Amazon CloudFront, AWS Application Load Balancer (ALB), Amazon API Gateway, and AWS AppSync, offering flexibility to organizations at all stages of application development and delivery.

## How WafCharm automates the AWS WAF rules

Automated managed service that strengthens AWS WAF security





## Case study: Adding agility and capability while reducing costs

A global manufacturing company needed a WAF that provided a high level of security and capability while lowering current costs. After extensively researching alternatives, it determined that WafCharm offered greater security capabilities than the current provider at half the price.

Its current system lacked agility. It took days to implement rule modifications—it also limited the number of times rules could be modified. Using WafCharm, the company was able to modify as many rules as needed and see updates take effect within one day. The company also had limited visibility into overall site security. The former solution generated a report every four months at an additional cost. WafCharm generates a monthly report at no additional cost.

Since switching to WafCharm, the company has received custom rule support on a regular basis and has found WafCharm to be easier to operate than its previous WAF provider. By implementing WafCharm, the customer simplified cyber security management, increased the overall level of security, and reduced costs by 50%.



## How WafCharm and AWS WAF benefit your business

As the implementation of APIs and web applications continue to grow, so do the number and sophistication of potential threats. AWS WAF and WafCharm add necessary layers of protection to your web applications and APIs on Amazon CloudFront. WafCharm automatically curates your WAF rules, ensuring your security is optimized and up-to-date while reducing the burden of configuring it yourself. On top of that, Cyber Security Cloud's security advisors provide automatic updates, expert industry knowledge, and top-tier customer support at no additional cost.

Start a **30-day free trial** of WafCharm

Discover **AWS WAF**

Learn more about **WafCharm**

## About Cyber Security Cloud

With an aim to create a secure cyberspace that people around the world can use safely, Cyber Security Cloud offers web application security services that leverage Cyber Threat Intelligence and AI technology. Based in Japan and the U.S., Cyber Security Cloud is available in over 70 countries and an AWS WAF Managed Rules Seller.

