CSC 2021 Research Insights Report

MANAGING MODERN WAF IN THE CLOUD

CSC
CYBER SECURITY CLOUD

Managing Modern WAF in the Cloud
TABLE OF CONTENTS

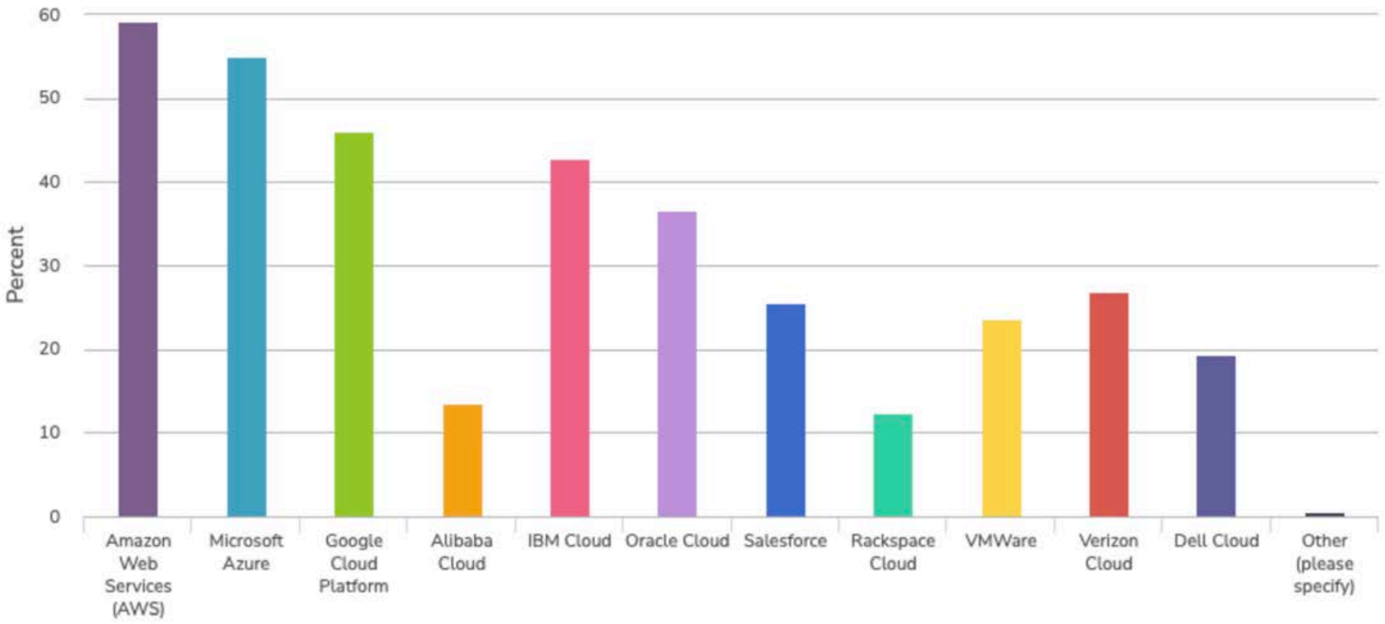
About This Report

A well managed web application firewall (WAF) has become an indispensable part of cybersecurity strategy for businesses of every size, across every vertical. It can prevent web-based attacks at the application layer and protect against exploits directed at application programming interface (API) vulnerabilities. Software developers and security engineers can tune a WAF to block malicious traffic—unencrypted (HTTP) or encrypted (HTTPS)—from entering a site and can prevent data from being extracted as a result of an intrusion.

By filtering traffic with AI-driven security technology that studies massive data sets, the most effective WAFs keep pace with emerging security risks and automatically apply immediate protection before hacker activity has a chance to impact business continuity. In the cloud, it's possible to apply a WAF in a way that protects all web applications and APIs across an organization. But what's possible and what's reality on the ground are two very different things, as is often the case in implementing infrastructure or, in truth, most intricate technologies.

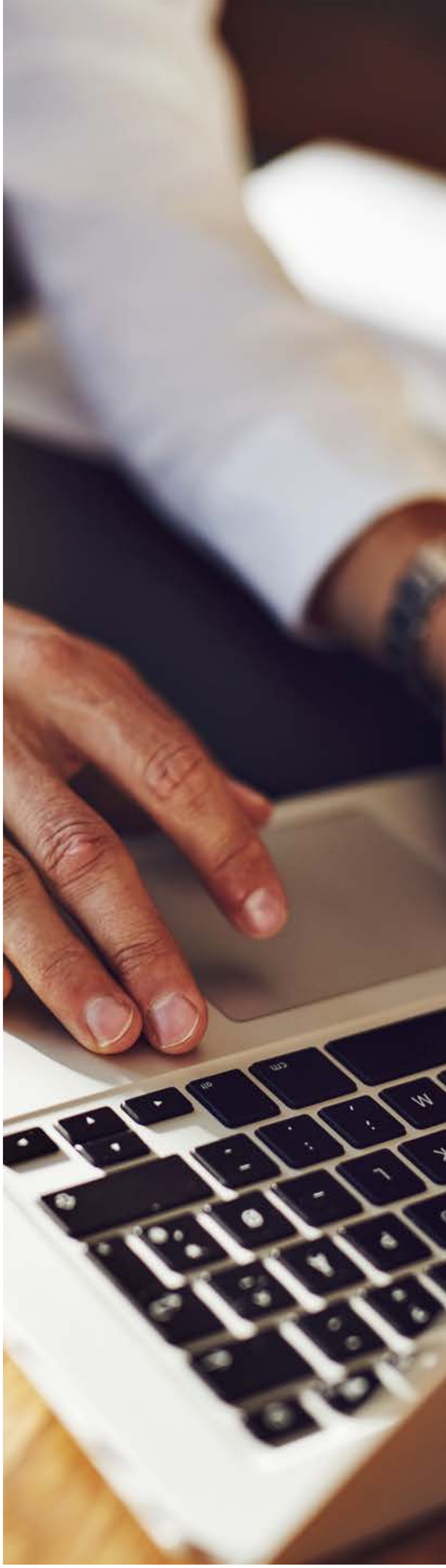
To better understand both the business necessity of using a modern WAF and the day-to-day challenges WAF management poses for those interacting with it, Cyber Security Cloud Inc. (CSC) surveyed 309 software developers and software engineers, 95% of whom work full-time in the IT or technology divisions of their companies. Their specific roles ranged from distinguished and principal software engineers to engineering and technical leads to software developers at every level working in front end, back end, and full stack positions—with 72% earning an income of $100K to $250K or more a year. Well educated, they represented multiple industries, including science, high tech, health tech, telecommunications and media, banking, financial services and insurance, construction, and education. And their companies ranged in size, with 11% of respondents working at startups and small businesses (<100 employees), 44% working at midsize enterprises (100 to 999 employees), and 45% working at large enterprises (1000 to 20,000+ employees).

All of those surveyed reported using cloud computing services at their companies, with 59% deploying Amazon Web Services (AWS), 55% Microsoft Azure, 46% Google Cloud Platform (GCP), 43% IBM Cloud, 37% Oracle Cloud, 27% Verizon Cloud, 26% Salesforce Cloud(s), 24% VMWare Cloud, 19% Dell Cloud, 14% Alibaba Cloud, 12% Rackspace Cloud, and 1% Apple iCloud.



Most respondents personally used cloud in their work, with 40% leveraging a public or private cloud model, 30% a hybrid environment, and 16% a multi-cloud deployment. Within those clouds, they collectively reported using 25 different categories of cloud and web application services—but 100% reported that their companies use WAF as part of their cybersecurity defenses.

This 2021 CSC Research Insights Report, Managing Modern WAF in the Cloud, focuses on a number of areas: web application security costs and the costs of cyber attacks; responsibility for cybersecurity and attacks; coping mechanisms developers use to deal with that responsibility; WAF's role in cybersecurity; developer skill levels and training with respect to WAF; and, finally, WAF pain points and what's needed to mitigate those.



Key Findings in WAF Management

The survey offers compelling findings about WAF management. Namely, the well educated and trained software developers who use it often find it overwhelming and time-consuming. They conveyed some of the frustration they feel managing cloud and web applications in a world constantly bombarded by cyber attacks. They also specified ways to alleviate the uncertainty in WAF management. Let's take a closer look.

Key findings convey developers' day-to-day concerns and challenges:

- A substantial majority of respondents, 64%, reported that their company has experienced cyber attacks, especially stolen data, ransomware attacks, and phishing.
- 94% said the cyber attacks were preventable.
- Almost 40% report the cost of an attack at hundreds of thousands to tens of millions of dollars and over half report preventative cybersecurity spending to be a hundred thousand to over 10 million dollars.
- 85% said that their own team or their boss was typically held responsible for successful cyber attacks.
- In this context, over a third have developed unhealthy habits from the impact of managing cloud or web applications, reporting that they drink more alcohol, oversleep, fight more with family or friends, grind their teeth at night, or overeat and eat unhealthy foods.
- Almost 75% of developers with an expert WAF skill level have a question at least once a week about WAF rules and, often, once a day.
- 72% of developers at all WAF skill levels said they are overwhelmed with the amount of WAF rules and conditions—and a telling 71% of WAF experts said the same thing.
- 94% would be interested in automated managed rules for WAF operation instead of managing the rules themselves.
- 91% think cloud or web application management should be a full-time job; 95% of expert-level WAF developers think the same.

Ever-evolving Cyber Threats and the Role of WAF

We live in a world where cyber attacks are ubiquitous and increasing in sophistication. The Center for Strategic & International Studies maintains a list of known attacks featuring government players and criminal hacker groups. The documented mayhem is constant, exposing a planet-wide state of cyber warfare causing data breaches and economic drain that can paralyze institutions and destroy lives. In 2021, ransomware attacks in the U.S., for example, continued to surge targeting all kinds of organizations – multinational IT firms, a global meat producer, companies responsible for critical energy and water infrastructure, health care organizations, universities, government agencies, and businesses in every vertical including one of the largest insurance companies in the U.S.

A major attack vector leveraged by ransomware and other kinds of cyber threats is web traffic, both encrypted and unencrypted. According to the Google Transparency Report, the percentage of encrypted web traffic across Google (its browsers and other products and services) has increased from 50% in January of 2014 to 90% in late 2017 to 95% from mid-2018 to the present. It's well established that hackers regularly hide malicious activity in encrypted traffic. Even as tools have evolved to chip away at the problem, many simply cannot closely inspect the volume of encrypted data interacting with an organization's applications, nor keep pace with hacker tactics preying on old and new software vulnerabilities alike.

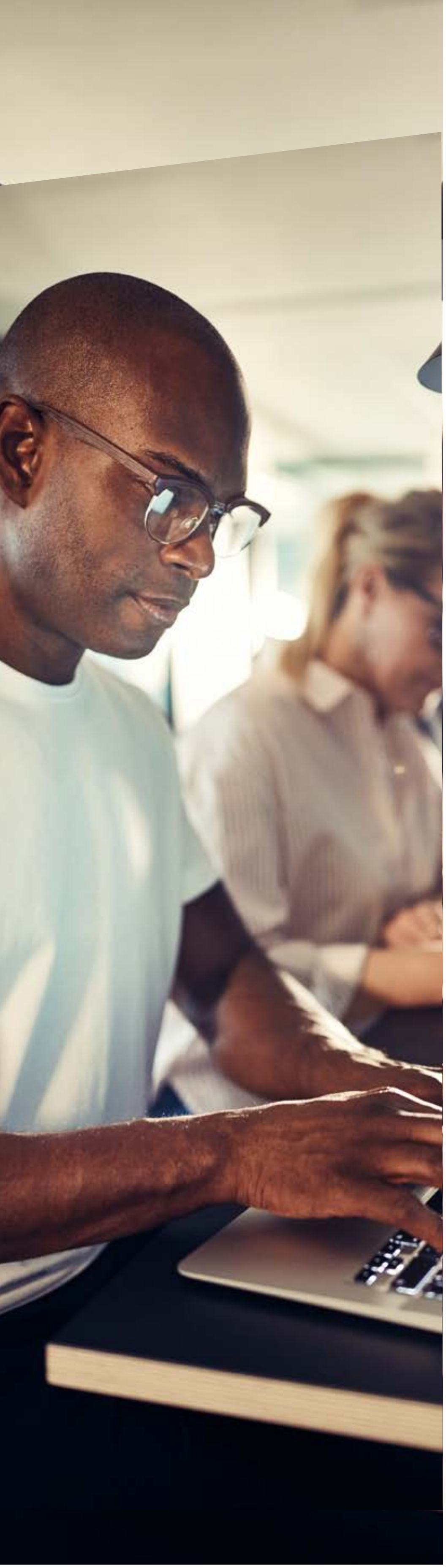
By controlling how traffic reaches web applications and APIs and vigilantly spotting attack patterns, a well designed WAF can block ransomware and address many of the OWASP Top 10 security risks, as well as other cyber threats like malicious bots and directory traversal that can consume costly resources, threaten data, and result in downtime. OWASP refers to the Open Web Application Security Project, a globally recognized, nonprofit endeavor that documents the most critical security risks to web applications.

Among the 2021 risks are: broken access control, cryptographic failures, code injection (SQL, NoSQL, OS command, Object Relational Mapping [ORM], LDAP, and Expression Language [EL] or Object Graph Navigation Library [OGNL]), cross-site scripting (XSS), security misconfiguration, and server-side request forgery. A WAF can address other known web application exploits that leverage tools like Apache Struts2, Apache Tomcat, Oracle WebLogic, WordPress, Drupal, Joomla!, and various implementation systems.

OWASP also publishes API security risks, as misconfigured APIs and third-party API calls in application logic continue to become growing sources of security breaches. Just as a WAF can be deployed on a cloud content delivery network (CDN) or application load balancer fronting web server instances, it can work with an API gateway to filter threats.

While a WAF is a key proactive defense in every organization’s drive to protect applications and sensitive data, it isn’t easy to successfully manage. That’s because its effectiveness lies in deploying scores of properly expressed rules that do the heavy lifting to filter a massive number of ever-evolving, malicious attack patterns.

The survey provided detailed information on developers who work hands-on in this arena—who manage cloud and web applications in a hostile cyberworld and who understand the need for WAF and its operational improvement.



The Survey: Application Security Spending and the Cost of Attacks

A substantial majority (64%) of the developers surveyed reported that their company has experienced cyber attacks, with the most prominent kinds of attacks including stolen data (69%), phishing (67%), and ransomware (58%). A whopping 94% of those surveyed said the cyber attacks were preventable.

The cost of those attacks ranged from mild to staggering, with 23% reporting that the cost was less than a thousand dollars, 38% reporting a cost of tens of thousands of dollars, 23% reporting hundreds of thousands of dollars, 8% at over a million dollars, and another 8% over 10 million dollars.

The survey found that almost 40% of developers reported the cost of attacks ranging from hundreds of thousands to tens of millions of dollars.

In addition to the costs associated with actual attacks, companies spent substantial sums on cloud and web application security in their efforts to prevent successful attacks. In broad terms, reported spending ranged as follows:

- 41% said their companies spent less than $100K
- 31% said their companies spent $100K to almost $1 million
- 10% said their companies spent $1 million to almost $10 million
- 7% said their companies spent $10 million to almost $100 million
- 3% said their companies spent $100 million to $1 billion or more
- 8% said they don’t know the level of spending

Within this wide range of company spending, the highest number of respondents (18%) reported that spending reached between $100K to almost $500K, and the second highest (13%) reported spending between $500K to almost $1 million, totalling 31%.

Spending below $100K fell into seven different tiers, with the 9% plurality in that group spending $50K to almost $100K.

The survey thus found that over half (51%) of developers reported preventative cybersecurity spending to be between $100K to $10 million or more.

Reported spending on WAF operation itself was also substantial:

- 33% said their companies spent less than $50K
- 11% said their companies spent $50K to almost $100K
- 24% said their companies spent $100K to almost $1 million
- 20% said their companies spent $1 million to $1 billion or more
- 12% said they don't know the level of spending

How Often Do Companies Pay for Web Security?

According to the developers surveyed, most companies paid for cloud or web application security fairly often, with almost 60% saying payment occurred every six months or more frequently:

- 15% said every month
- 19% said every three months
- 25% said every six months
- 32% said every year
- 6% said every two years
- 3% said every three to five years

The frequency of WAF spend tracked the frequency of cloud and web application security spend fairly closely, with 57% saying payment occurred every six months or more frequently:

- 18% said every month
- 17% said every three months
- 22% said every six months
- 31% said every year
- 6% said every two years
- 6% said every three to five years

Whose Job Is It Anyway?
The Burden of Responsibility

While 65% of developers said that managing cloud or web applications was their only responsibility and 35% indicated additional responsibilities, 91% said this work *should* be a full-time job. Among developers with expert-level WAF skill, 95% thought the work of managing cloud or web applications *should* be a full-time job.

When it came to internal or external management of security, 92% of developers indicated that their internal IT department managed their security environment; only 8% indicated that a third-party vendor managed it.

The survey showed that bearing the burden of responsibility for successful cyber attacks was part of many developers' lives: 54% said that their own team was typically held responsible; 31% said their boss was held responsible; and 15% said a third-party security solution provider was held responsible.

With the survey finding that 85% of developers said that their own team or their boss was typically held responsible for successful cyber attacks, perhaps the coping mechanisms many employed were not surprising. Over a third (34%) of respondents have developed unhealthy habits from the impact of managing cloud or web applications, reporting that they drink more alcohol, oversleep, fight more with family or friends, grind their teeth at night, or overeat and eat unhealthy foods. Others found solace in healthier habits: 43% worked out, 18% meditated, and 5% said they pray.

WAF-specific Responsibilities, Skill Levels ... and Pain Points

Survey respondents shared who actually operates their company's WAF, with 77% indicating that developers or other in-house technical roles are responsible and 76% specifying that they themselves are the personnel who manage WAF. Of the latter, 85% report that they manage it either daily (37%) or weekly (48%).

Additionally, 19% of the developers indicated that managed security service providers (MSSPs) operate their company's WAF and 4% said consulting companies or others do this. With less than one-quarter of companies relying on MSSPs, the need for in-house WAF expertise is high.

Self-reported skill level with WAF ranged from beginner (15%) to intermediate (38%) to expert (47%). Respondents' years of experience using WAF was fairly even across time frames that spanned less than six months through 10 years of experience, with a handful of users reporting 11 to 15 years of experience.

Overall, 84% of respondents had training on WAF and 16% had no training. Of those with training, 54% received their training from a cloud or web application provider, 25% received in-house training, and 21% were trained outside of their company and/or the provider.

Among those who reported expert-level skill with WAF, almost all (98%) indicated they had received training. The vast majority (85%) of those with intermediate-level WAF skill reported receiving training, but less than half (39%) of WAF beginners reported receiving training. Most of the training that beginners received happened in-house, while a majority of training reported by intermediate- and expert-level WAF users happened through a cloud or web application provider.

The survey revealed that WAF rules are a pivotal pain point in WAF management. For the 76% of developers surveyed who themselves operate WAF, questions about WAF rules were common:

- 21% have a question once a day
- 48% have a question once a week
- 23% have a question once a month
- 8% have a question less than once a month or never

Thus, 69% of developers at all skill levels have a question at least once a week or more often about WAF rules. Even more compelling is that almost 75% of developers with expert-level WAF skill have a question at least once a week about WAF rules and, often, once a day, according to the survey.

A powerful majority, 72%, of developers at all WAF skill levels said they are overwhelmed with the amount of WAF rules and conditions—and a telling 71% of WAF experts said the same thing. The solution was clear: 94% of developers would be interested in automated managed rules for WAF operation instead of managing the rules themselves.

The survey also compiled specific data about AWS users among the developers surveyed, 59%, versus non-AWS users. Regarding questions about WAF, AWS users answered as follows:

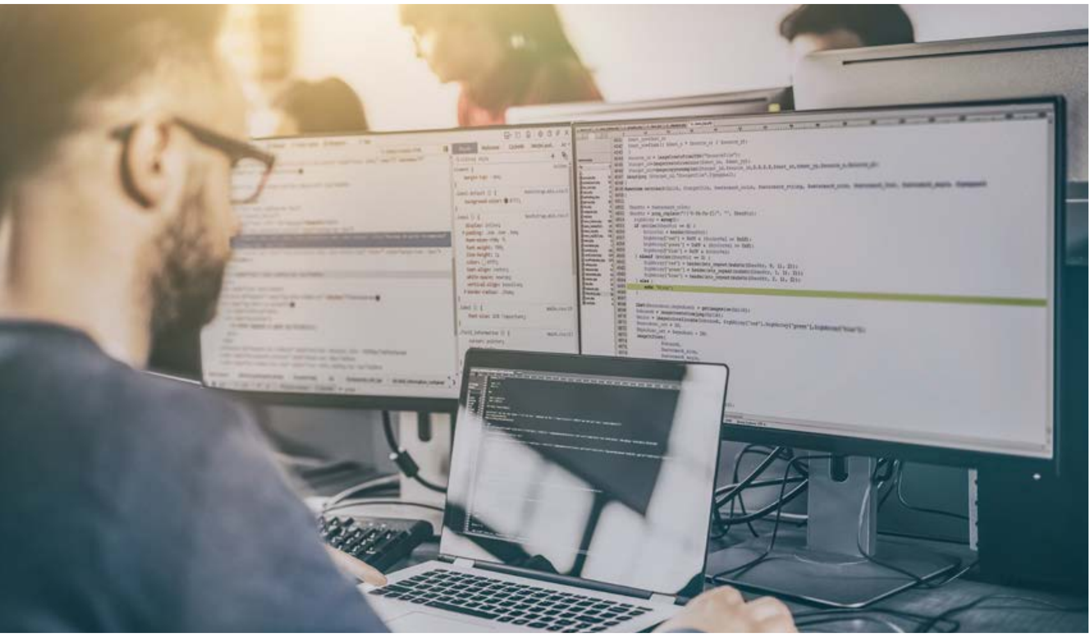
-
- 23% have a question once a day
- 50% have a question once a week
- 21% have a question once a month
- 6% have a question less than once a month or never

Non-AWS user percentages were close, with 19% having a question once a day, 45% once a week, 26% once a month, and 10% less than once a month or never.

Similar to the developer responses overall, 74% of AWS users are overwhelmed with the amount of WAF rules and conditions; 70% of non-AWS users report the same. And 96% of AWS users would be interested in automated managed rules for WAF operation instead of managing rules themselves; 92% of non-AWS users said the same.

It's worth recalling that the developers surveyed were a well educated group, with 49% having earned a Bachelor's degree and another 39% having earned a Master's degree or higher level of degree. With respect to infrastructure environments, the developers indicated comfort with the cloud. They reported that they most trust cloud (31%), hybrid cloud (30%), or a multi-cloud model (18%)—with only 21% reporting they trust an on-premises environment most.

The data here, then, point to some clear truths about WAF in today's complex cyber threat landscape. Well implemented WAF rules are pivotal for preventing attacks, but they are very difficult for humans, even technically savvy ones, to fully manage—and even with the advantages cloud computing offers. Keeping up with all of the web and API vulnerabilities and rule details necessary to detect attack patterns, and acting with the inhuman speed necessary to stop new forms of attack, require an automated rules solution.



WafCharm for AWS and Future-Forward Cybersecurity

The survey strongly points to the fact that a potent, developer-preferred WAF requires automated rules management. CSC's WafCharm offers that. WafCharm automatically optimizes rule operations and eliminates the burden of complex rule creation to help address web-related cyberattacks.

Leveraging one of the most sophisticated cyber threat intelligence and research teams in the world, WafCharm uses threat intelligence analytics that employ extremely fast vulnerability response speeds. With uniquely robust AI-driven functionality, WafCharm learns from petabytes of data—spotting known and zero-day threats and greatly reducing wasted time and resources on false-positives. The solution is effective, affordable, and easy-to-use for global AWS WAF rules management.

WafCharm only takes a few minutes to implement, then all AWS WAF operations are automated, including the handling of new vulnerabilities that surface around the world and may impact customer deployments anywhere. WafCharm is built for ease of use, offering:

- Easy installation and operation – It's not necessary to install any special equipment or switch a DNS. WafCharm automatically selects the optimal rules/signatures, but allows customers to fix those that they do not want changed automatically.
- No required customer correspondence – Security experts monitor customer deployments and quickly create and apply new rules/signatures when dealing with new vulnerabilities in the threat landscape.
- Optimal protection for everyone – For any deployment leveraging AWS WAF, Wafcharm enables automated selection of optimal rules/signatures.
- Better security with hundreds of signatures – Since there is a possibility of leakage with limited numbers of rules, WafCharm rematches access data with hundreds of rules/signatures; attack sources identified by rematching are blacklisted automatically.

- Robust reporting and notifications – Via AWS Kinesis Data Firehose, S3, and Lambda, WafCharm support can help customers generate reports from the WafCharm management screen.

Cybersecurity is the purview of all software developers. The defense of applications and data is deadlocked with the growth and constancy of cyber attack. Even the most competent technical professionals must have AI-driven systems that learn and grow at an extraordinary pace to support their work in order to future proof today's and tomorrow's applications for business, government, and quality of life.

Contact Information:
Sales Office
csc_us@cscloud.co.jp
Cyber Security Cloud Inc.
700 S. Flower Street Suite 1000
Los Angeles, California 90017