PRISMA® CLOUD | paloalto® NETWORKS

Raising the Bar for Web Application and API Security

Cloud native applications continue to grow and are being packaged using containers, serverless functions and microservices on a variety of technology stacks. Rather than leveling out over time, these complex architectures are only going to become more prevalent. Securing the web applications and APIs that underpin these complex architectures has traditionally been a challenge for application security and DevOps teams. The web applications and APIs are continually changing, and existing web security solutions lack needed coverage.

In response, Palo Alto Networks offers best-in-class Web Application and API Security (WAAS) as part of the Prisma Cloud platform. In this paper, we offer a quantitative analysis of the module and compare it to other solutions in the industry. In doing so, we demonstrate Prisma Cloud's WAAS superior accuracy.

Measurement 101: Cybersecurity Solution Accuracy

The most basic requirement for a web application and API protection solution is to block web-based attacks such as SQL injection, cross-site scripting, and local file inclusion. However, cybersecurity solutions should never be evaluated based solely on how good they are at blocking attacks. If that were the case, the best cybersecurity solution would probably be a disconnected ethernet cable—not connected to anything. Unfortunately, the flip side of this drastic approach would probably be a significant loss of legitimate business.

The best comparative tests take into account multiple standard binary classification accuracy factors related to cybersecurity when evaluating solution competence. In this paper, we consider:

- **False positives (FP)**—legitimate activity incorrectly flagged as malicious
- **False negatives (FN)**—malicious activity not detected
- **True positives (TP)**—malicious activity correctly detected as malicious
- **True negatives (TN)**—legitimate activity correctly detected as legitimate

Any analysis that tries to assess and compare the accuracy of cybersecurity solutions must consider all four factors to allow users and buyers to choose which solution best fits their use case. After all, not all use cases are the same; some might prefer a different balance between business continuity and security protection levels.

These four accuracy factors can be measured using two statistical concepts known as precision and recall:

- **Precision** is the fraction (or percentage) of flagged requests that were actually malicious. In other words, precision describes how prone a security control is to false positives. A higher precision value means the control generates fewer false positives.
- **Recall** is the fraction (or percentage) of attacks that were flagged correctly. A higher recall value means the solution is appropriately detecting attacks.

Using the aforementioned four accuracy factors, it is also helpful to calculate a single accuracy score that appropriately quantifies a solution's overall abilities. One such score is the Matthews Correlation Coefficient (MCC), or phi coefficient. The MCC formula results in a single MCC value.

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP \times FP)(TP + FN)(TN + FP)(TN + FN)}}$$

Figure 1: The formula for calculating the Matthews Correlation Coefficient

In essence, an MCC value of **+1.0** means the solution is right all the time—it always detects malicious activity and always allows legitimate activity. An MCC value of **-1.0** means the solution is wrong in every decision it makes—legitimate activity is always blocked, and malicious activity is never blocked. Lastly, an MCC value of **0.0** means the solution is no better than merely applying a random choice.

Now that we know what to measure when evaluating a cybersecurity solution, let's apply this to our WAAS solution.

Accuracy Measurement: Web Application and API Security

In the context of web application security, a false positive means a legitimate HTTP transaction (e.g., a legitimate user's form submission) was incorrectly blocked by the protection mechanism. A false negative means a web-based attack, such as an SQL injection attempt, was not flagged by the protection mechanism. True positives indicate web-based attacks that were correctly flagged, and true negatives mean legitimate user traffic was allowed to reach the web application or API endpoint.

Based on this, **precision**, in the context of web application security, portrays the level of false positives generated by the security control. **Recall**, then, describes how effective the security control is at detecting attacks.

Naturally, we want the precision, recall, and MCC values to be as high as possible. To gain this assurance, we must have a way to test these values.

Measuring False Negatives and True Positives

To measure how well a solution deals with false negatives and true positives, all you have to do is prepare a vast arsenal of attack test cases, covering all known attack vectors. Such an arsenal can be compiled by collecting real-world attack traffic, recording hacker automation tools, and scraping hacker site content.

Once the arsenal is ready for launch, you only have to deploy the protection mechanism in front of a web application and fire away. Any attack that is blocked denotes a true positive, and a missed attack denotes a false negative.

Measuring False Positives and True Negatives

This is where things become tricky. You can measure false positives by protecting a web application and then inspecting whether legitimate user traffic triggers a security control. Such an approach requires that you define how much traffic is enough. Moreover, the statistics collected will only be relevant for that specific web application.

A slightly different take on this approach would be to record a large amount of legitimate traffic from as many real-world web applications and APIs as possible, from many different types of applications (e.g., mobile app backend APIs, e-commerce websites, CRMs, marketing websites). Once you've collected a diverse test set of legitimate traffic, the traffic is replayed through the tested protection mechanism. Every security trigger from this set denotes a false positive, and every request that is allowed to reach the application denotes a true negative.

With all four accuracy factors calculated, you can then calculate the MCC score and assess the solution's overall accuracy.

It should be noted that this approach is not exactly new. The author developed a framework for testing the accuracy of web application firewalls in 2013 and presented it at the NYC OWASP conference that year.

Accuracy Test: Prisma Cloud WAAS Module

For our accuracy test, we collected a set of more than 200,000 legitimate HTTP transactions from a diverse set of top web applications, websites, and web APIs. In addition, we compiled a rich arsenal of more than 5,000 unique web attack vectors, which cover every OWASP Top 10 category—and beyond. We deployed the WAAS module and ran the scenarios.

The overall MCC score calculated for the Prisma Cloud WAAS module was **0.956**.

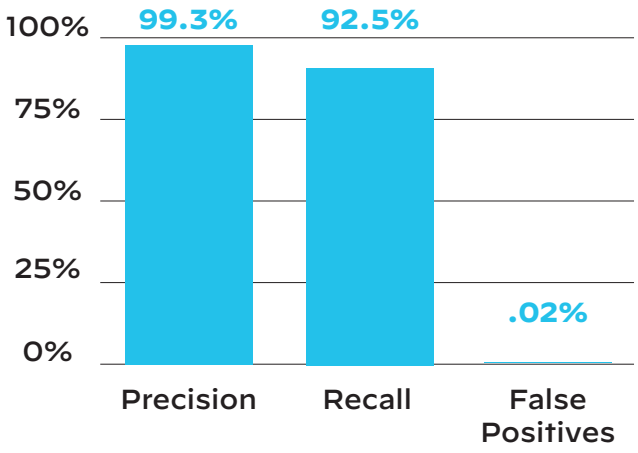

Figure 2: Prisma Cloud WAAS module—precision, recall, and false positives

Industry Comparisons

While these statistics are interesting, they are not entirely meaningful unless you compare the module's accuracy to other industry-leading solutions. Using the same testing methodology, we ran the same set of tests against six other solutions:

- Two leading web application firewall (WAF) solutions and services
- One open source WAF solution
- Two leading cloud service provider (CSP) WAF solutions
- One runtime application self-protection (RASP) solution

Table 1 shows the compiled results, comparing the Prisma Cloud WAAS module with related solutions.

Table 1: Prisma Cloud WAAS Module Compared to Related Solutions

Solution	Precision	Recall	False Positives	MCC
Prisma Cloud WAAS Module	**99.3%**	**92.5%**	**0.02%**	**0.956**
WAF #1	65.5%	91.1%	1.61%	0.764
WAF #2	87%	85.9%	0.43%	0.866
Open Source WAF	91.3%	91%	0.29%	0.908

Table 1: Prisma Cloud WAAS Module Compared to Related Solutions (continued)				
Solution	**Precision**	**Recall**	**False Positives**	**MCC**
CSP WAF #1	57.6%	83.5%	2%	0.681
CSP WAF #2	61.4%	91.3%	0.85%	0.729
RASP Solution	79.9%	50.1%	0.85%	0.614

Prisma Cloud WAAS: Superior Accuracy Beyond Doubt

We have examined the optimal methodology for testing the accuracy of a Web Application and API Security solution. We learned that it is not enough to discuss how strict a solution is or how many attacks it can block if we don't factor in its behavior on legitimate traffic and its level of false positives. Using the testing methodology presented, we compared the accuracy statistics for the Prisma Cloud WAAS module against other leading solutions, The statistics speak for themselves and clearly demonstrate its superior accuracy.

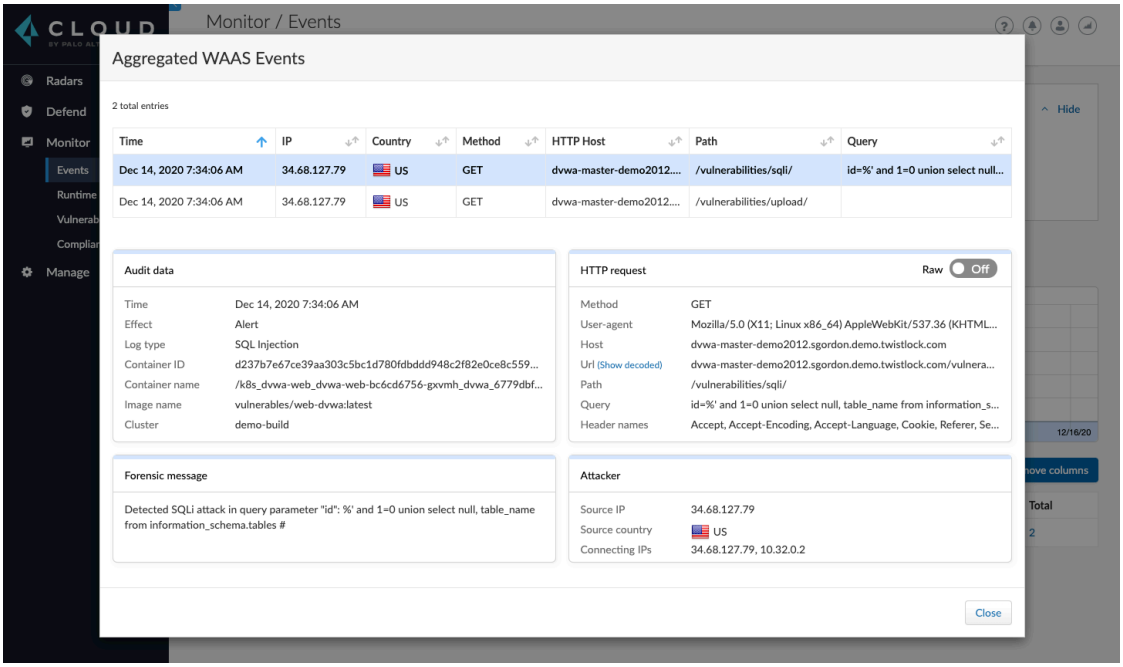

Figure 3: Aggregated WAAS audit details in Prisma Cloud

About Prisma Cloud by Palo Alto Networks

Prisma® Cloud is the industry's most complete Cloud Native Application Protection Platform (CNAPP), with a vision for unmatched, integrated cloud security to ensure that cloud environments and cloud native applications are secure—throughout the development lifecycle and across hybrid and multi-cloud environments.

The integrated approach eliminates the security constraints around cloud native architectures—rather than masking them—and breaks down security operational silos across the entire application lifecycle, allowing application security and DevSecOps/DevOps teams to automate security to meet the changing needs of cloud native architectures.

To learn more, you can visit us online or watch a demo now.

paloalto® NETWORKS | Cybersecurity Partner of Choice

3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087