SecureIQlab®

Cloud WAAP v3.0

CyberRisk Validation Comparative Report Cloud Web Application and API Protection (WAAP)

Language:	**English**
Published:	**9 May, 2024**

Contents

1. Introduction

SecureIQLab conducted testing for 15[1] Leading Cloud WAAP solutions. Unlike tests from any other organization, SecureIQLab combines security efficacy metrics with operational efficiency assessment metrics, which are critical in securing and improving enterprises' overall security investment strategy. SecureIQLab is dedicated to advancing Cloud WAAP Solutions to ensure they offer the essential protection and operational optimization required in modern cybersecurity environments. These results are for Cloud WAAP v3.0 of the SecureIQLab Cloud Web Application and Application Programming Interface (API) CyberRisk Validation Methodology. It is the cybersecurity industry's "first of its kind" Application Programming Interface (API) validation performed against the modern-day Cloud Web Application Firewall solutions.

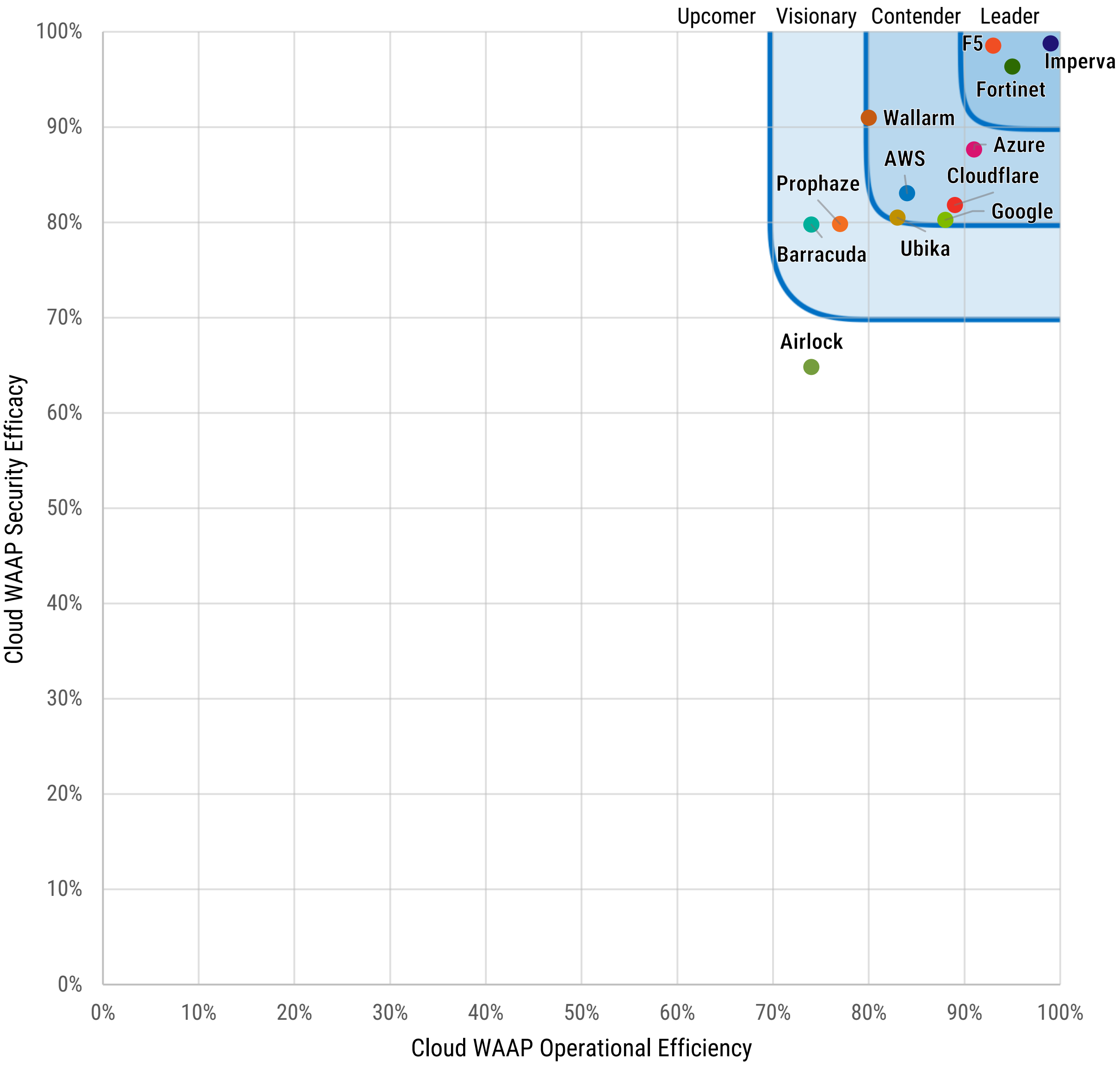


Figure 1. 2024 Cloud WAAP CyberRisk Ripple

[1] Testing was attempted on a total of 15 Cloud WAAP solutions. Please click here for details.

The 2024 Cloud WAAP v3.0 CyberRisk Ripple[2] highlighted above in Figure 1 captures the security efficacy (represented in the Y-Axis) versus operational efficiency (represented in the X-axis) metrics of the different enterprise-class cloud WAAP solutions validated against SecureIQLab Cloud WAAP v3.0 Methodology[3].

2. SecureIQLab Cloud Web Application & API Protection CyberRisk Ripple

This comparative report provides an overview of the results for all tested vendors. Vendors that completed testing are grouped alphabetically within the ranking in Figure 2. The four rankings vendors fell into are Leader, Contender, Visionary, and Upcomer. These rankings are derived from the Cloud WAAP CyberRisk Ripple in Figure 1 in the previous section. Test results have necessarily been simplified and presented for review in a summary format. In writing this report, SecureIQLab has made extensive efforts to guarantee the accuracy of the results while straightforwardly presenting them. There are also individual reports for each vendor, which are available here.

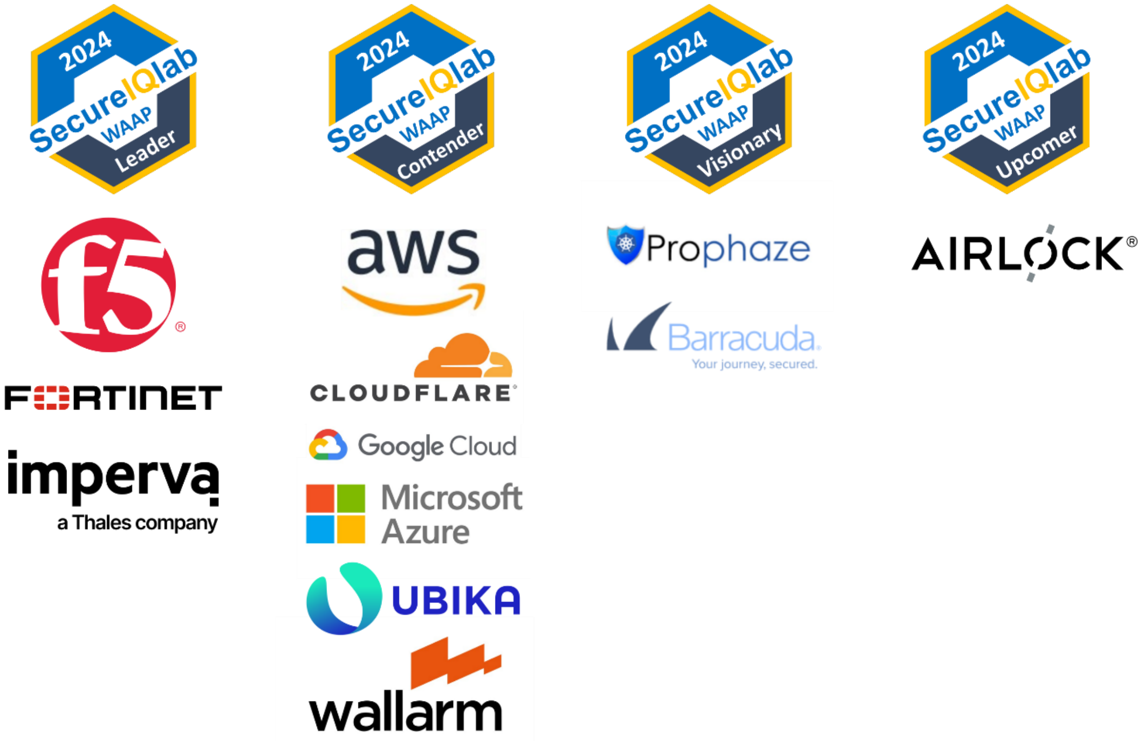


Figure 2. SecureIQLab WAAP v3.0 Security Vendors

[2] Please click here details on the SecureIQLab WAAP CyberRisk Ripple.

[3] SecureIQLab Cloud WAAP v3.0 Methodology

Vendor Name	Cloud WAAP Product Name	Overall Security Efficacy Score (%)	Overall Operational Efficiency Score (%)	CyberRisk Ripple Category
Airlock	Airlock Secure Access Hub – Airlock Gateway	64.8%	74.4%	Upcomer
Akamai	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
Amazon AWS	AWS WAF & Shield	83.1%	83.8%	Contender
Barracuda	Barracuda Application Protection	79.8%	73.5%	Visionary
Cloudflare	Cloudflare WAF	81.8%	88.9%	Contender
F5	Web App & API Protection	98.5%	93.2%	Leader
Fastly	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
Fortinet	Fortiweb Web Application Firewall WAF VM	96.4%	94.9%	Leader
Google	Google Cloud Armor & Apigee API Management	80.3%	88.0%	Contender
Imperva	Web Application Firewall	98.8%	99.1%	Leader
Microsoft Azure	Azure Web Application Firewall	87.7%	90.6%	Contender
Prophaze	Prophaze Hybrid WAF 3.0	79.8%	76.9%	Visionary
Radware	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
Ubika	UBIKA WAAP Cloud	80.5%	82.9%	Contender
Wallarm	Wallarm Advanced API Security	91.0%	80.3%	Contender

Table 1. SecureIQLab Cloud WAAP v3.0 Results Summary

Table 1 presents the vendor results in alphabetical order with their overall percentages and their placement category within the SecureIQLab Cloud WAAP v3.0 CyberRisk ripple.

Overall Result Summary: Among the 12 validated security solution vendors, ***F5 Networks, Fortinet & Imperva*** had exceptional security efficacy & operational efficiency scores in all the primary enterprise categories, placing them in the **Leader** category, while ***Amazon AWS, Cloudflare, Google, Microsoft Azure, Ubika*** & ***Wallarm*** had above average scores overall placing them in the **Contender** category. ***Barracuda Networks*** and ***Prophaze*** had good, compelling solutions, placing them in **Visionary**, while ***Airlock*** was placed in the **Upcomer** due to their below-average overall scores.

3. Security Efficacy Comparative Review

Every cloud WAAP evaluated in this test was subjected to 11 different categories of more than 30 real-world-based operational scenarios targeting small-to-medium businesses and enterprises. Over 3500 validated attacks were used to encompass these scenarios and categories. The testing performed by SecureIQLab carries on our tradition of innovation and improvement. SecureIQLab will continue to add attack libraries and other relevant operational metrics in future iterations of this test.

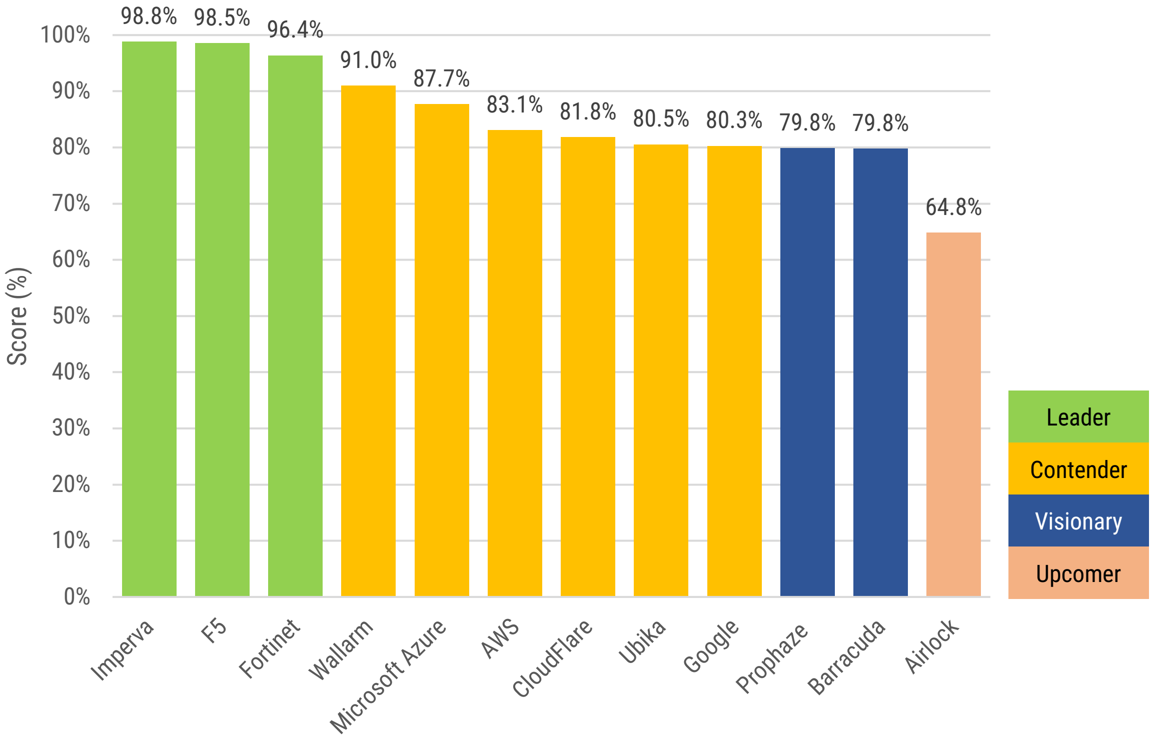


Figure 3. Overall Cloud WAAP Security Efficacy Results

Figure 3 above provides an overview of the SecureIQLab findings during the security validation of the 12 Cloud WAAP solutions with the overall average security score of 85%.

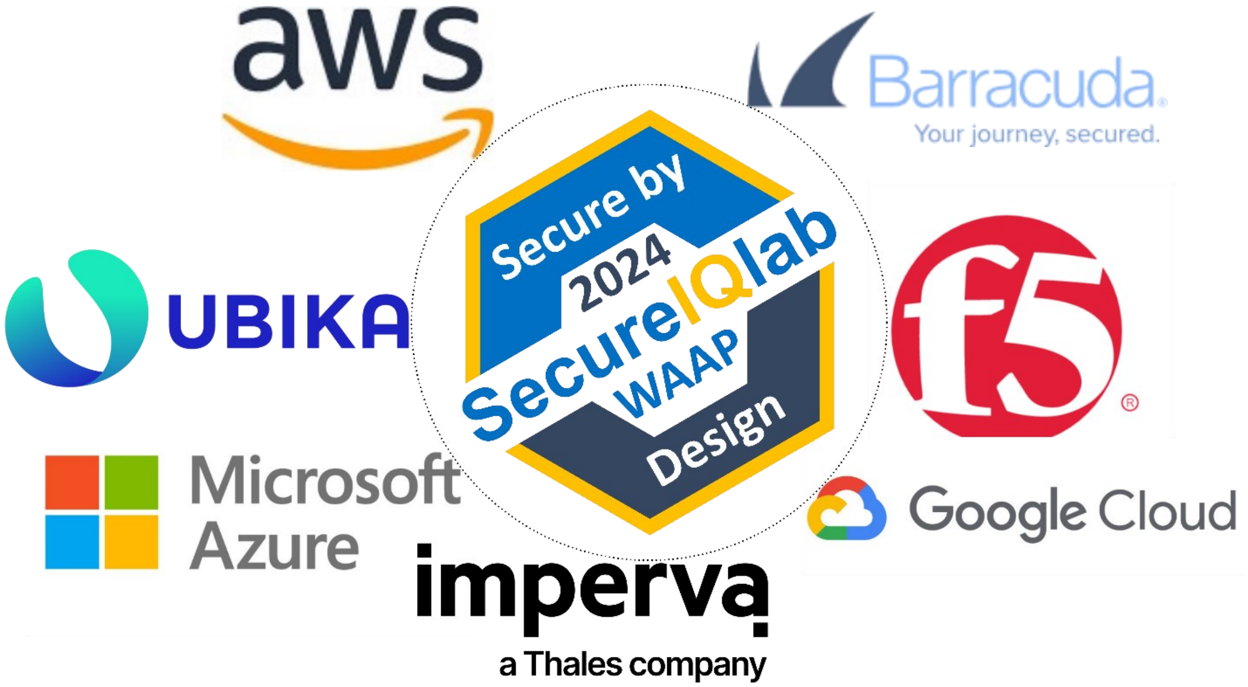
3.1 SecureIQLab 'Secure-by-Design' Cloud WAAP v3.0 Vendors

Security solutions, regardless of their deployment method, should not increase the attack surface of the environments that they are designed to protect. Additionally, privileges granted to security solutions should not be exploitable by threat actors. SecureIQLab has also assessed the security of the cloud WAAP product itself.

All 12 of the Cloud WAAP Security Solutions were tested against 11 vulnerability assessment techniques that are commonly used to assess that WAAP systems are built to reasonably protect against cyber-attacks as recommended by Cybersecurity and Infrastructure Security Agency (CISA). Furthermore, this assessment also represents secure design outcomes. Please refer to the Cloud WAAP Security Solutions individual test report published here, which provides the details of our findings. Seven out of the 12 WAAP solutions tested passed the WAAP Vulnerability Assessment with a score of 100%.

SecureIQLab rated Cloud WAAP security solutions vendors as "Secure-by-Design" only if they earned a perfect score in the WAAP vulnerability assessment security category.

.



3.1. OWASP Top 10 Validation

The OWASP Top 10 lists are assembled by security experts from across the globe and describe the most critical web application and application programming interface vulnerabilities The order of these lists is based on vulnerability frequency, severity, exploitability, and detectability. SecureIQLab testing is based on the most recent iterations of the OWASP Top 10 Web Application Security Risks—2021 and OWASP Top 10 API Security Risks—2023.

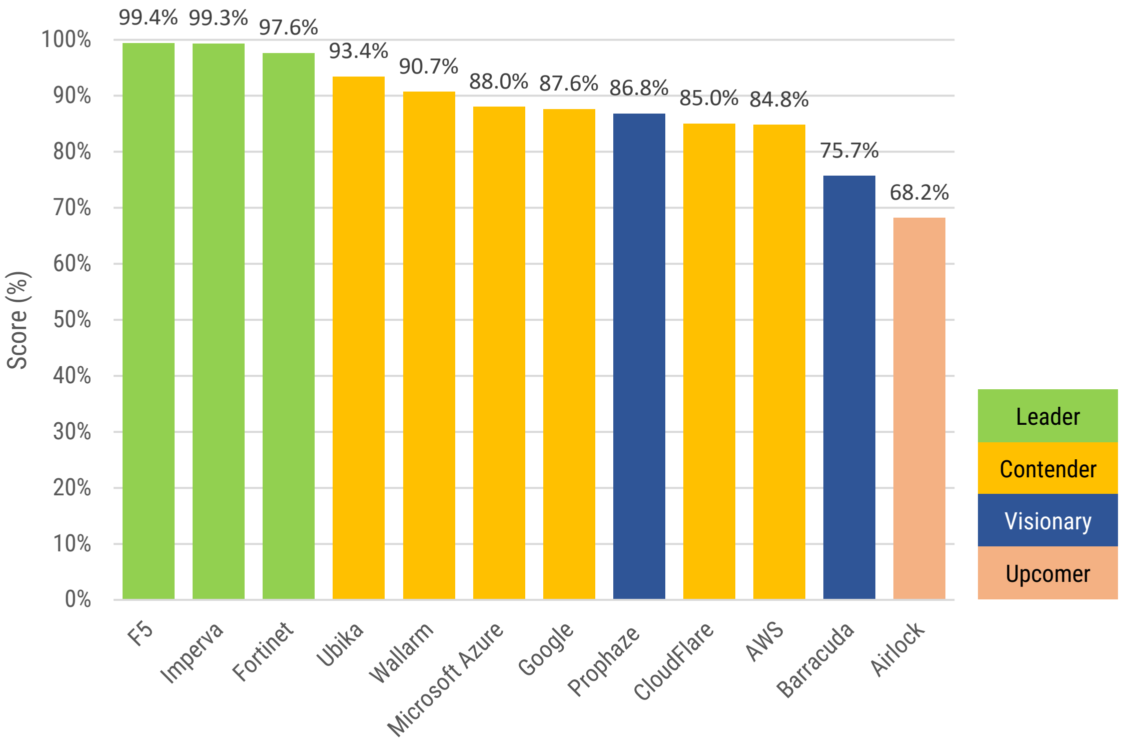


Figure 4. Overall OWASP Vulnerability Testing

Figure 4 above provides the overall OWASP security scores from all 12 vendor results from these tests. The Cloud WAAP solutions were tested against 9 of the OWASP Top 10 vulnerabilities. The OWASP A08:2021 – Software and Data Integrity Failures vulnerability was not included in testing because it relates to coding and infrastructure practices that are outside the scope of WAF security. For detailed explanations of these attacks, please reference the OWASP Top 10.

3.2. Advanced Threat Coverage

The results of advanced threat coverage represent threats that are not covered by OWASP Top 10 but are sophisticated and relevant enough for every WAAP solution to provide coverage. Figure 5 below highlights the combined Bot Attacks, Layer 7 DoS Attacks, Resiliency, and WAAP Vulnerability Assessment scores for all 12 vendors.

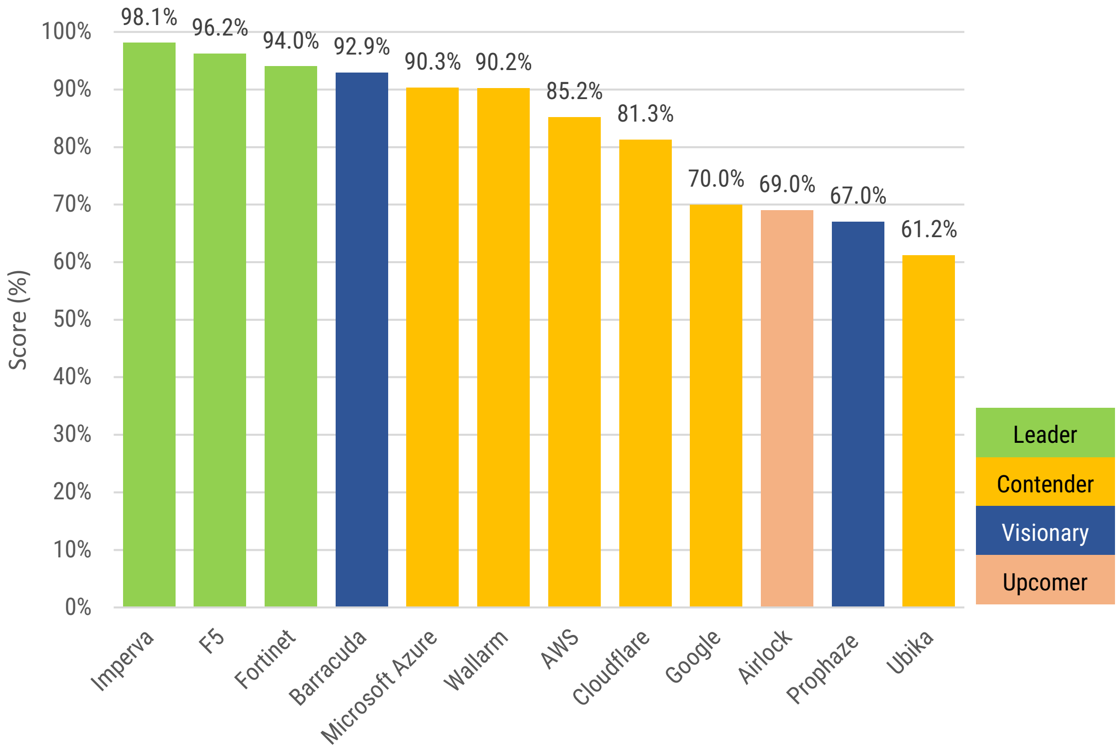


Figure 5. Overall Advanced Threat Score

For more details on each of the above threat categories, please refer to the Cloud WAAP Security Solutions individual test report published here.

4. Operational Efficiency

Operational efficiency in deploying, managing, and utilizing WAAP solutions is critical for modern enterprises. WAAP solutions that provide security with a high operational efficiency optimize resource allocation minimize the burden on infrastructure and reduce operational costs. WAAPs must be easy to deploy, manage, and provide the necessary controls to amplify security without interrupting business workflow. Prioritizing WAAP solutions that have high operational efficiency, or in other words, require minimal resources, is critical for organizations looking to protect digital assets effectively while keeping pace with today's rapidly shifting business environment.

SecureIQLab validated WAAP operational efficiency in five areas of validation with a total of 39 features and functions validated. These five areas include Ease of Deployment, Ease of Management, Ease of Risk Management, Scalable & Elastic Capabilities, and Logging& Auditing Capabilities. Figure 6 below provides an overview of the operational efficiency findings for all the Cloud WAAP Security Solutions. For additional details about each security solution and the operational efficiency categories, please refer to the Cloud WAAP Security Solutions individual test report published here.

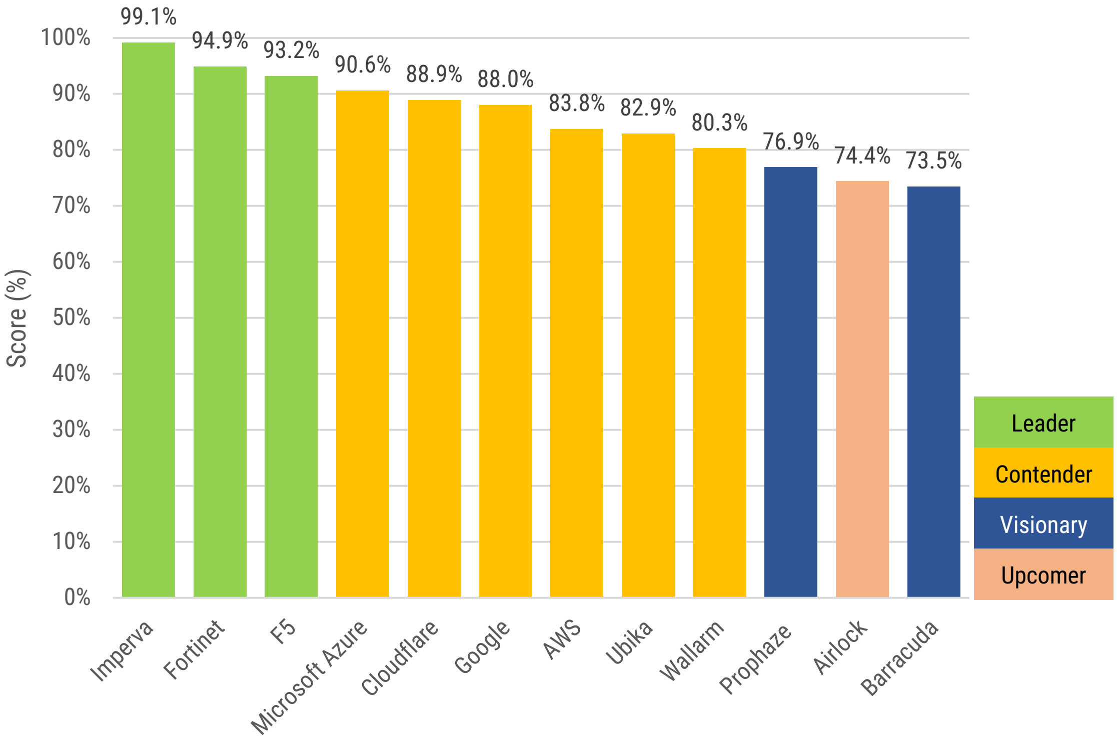


Figure 6. Overall Operational Efficiency Score

Most of the Cloud WAAP security vendors had above average (86.9%) operational efficiency capabilities in the five major validated categories of operational efficiency, as highlighted in Table 2 below.

Cloud WAAP Operational Efficiency Categories	Ease of Deployment	Ease of Management	Ease of Risk Management	Scaling and Elastic Capabilities	Logging and Auditing Capabilities
Airlock	81%	78%	72%	53%	76%
Ubika	67%	86%	83%	80%	100%
Wallarm	78%	78%	94%	80%	76%
AWS	74%	89%	83%	80%	90%
Fortinet	89%	97%	94%	100%	95%
CloudFlare	89%	92%	89%	80%	90%
F5	100%	92%	94%	80%	95%
Imperva	100%	97%	100%	100%	100%
Barracuda	89%	61%	67%	80%	76%
Prophaze	96%	75%	78%	53%	71%
Google	85%	89%	83%	100%	86%
Microsoft Azure	96%	92%	72%	100%	90%

Table 2. Overall Operational Efficiency Category Results

5. False Positive Avoidance

Cloud WAAPs need to allow business-related transactions while blocking malicious activity. The false positive rate is important because false positives interfere with the operation of the business. Policies need to be adjusted to minimize false positives. Blocking legitimate user activity constitutes a false positive, increases the operational burden for the enterprise, and requires additional tuning to correct it.

Properly tuned security devices will not detect benign traffic as malicious. More than 6500 false positive test cases were used to validate that the product under test (PUT) would not block simulated consumer purchases. These test cases simulated users that would browse the web application normally while protected by the cloud WAAP.

The highest *False Positive Avoidance Score* of the group of tested vendors in this category was 100.0%, and the lowest score was 99.90%, with all 12 Cloud WAAP security solutions performing remarkably well.

6. Conclusion

The Cloud WAAP security vendors had an average security efficacy score of 85.50% and operational efficiency score of 86%. The overall *Security Scores* have significantly improved compared to the previous Cloud Web Application Firewall v2.0 group test validation in 2023. We are releasing the first-of-its-kind Cloud WAAP v3.0 report by measuring "Secure-by-Design" and what it means to the enterprise. 7 of the 12 participating vendors were rated by SecureIQLab as such. This Cloud WAAP v3.0 comparative report also twists heads around by focusing on operational efficiency to make enterprises make educated decisions on how technology improves or keeps pace with organizational productivity, enabling them to make informed decisions.

7. Cloud WAAP 2024 Statistical Analysis

At the conclusion of testing, the Cloud WAAP 2024 test results were analyzed statistically. Table 3 provides the Matthews correlation coefficient, precision, and recall for the test results.

Vendor	MCC	Precision	Recall
Airlock	0.94	1.00	0.94
AWS	0.88	1.00	0.88
Microsoft	0.92	1.00	0.92
Barracuda	0.84	1.00	0.85
Cloudflare	0.91	1.00	0.91
F5	1.00	1.00	1.00
Fortinet	0.97	1.00	0.97
GWAF	0.92	1.00	0.92
Imperva	0.99	1.00	0.99
Prophaze	0.96	1.00	0.96
Ubika	0.97	1.00	0.97
Wallarm	0.94	1.00	0.94
Average	0.94	1.00	0.97

Table 3. Cloud WAAP 2024 Test Statistics

To better understand these performance metrics, Table 4 provides definitions for the variables used in the calculation of these metrics.

Variable	Meaning	Definition
TP	True Positive	# Benign Allowed
FP	False Positive	# Benign Blocked
FN	False Negative	# Attacks Missed
TN	True Negative	# Attacks Blocked

Table 4. Definition of Variables

Calculation of the Matthews correlation coefficient is provided in Equation 1 below.

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

Equation 1. Matthews Correlation Coefficient Calculation

Calculations of precision and recall are provided in Equation 2 and Equation 3, respectively.

$$Precision = \frac{TP}{TP + FP}$$

Equation 2. Precision Calculation

$$Recall = \frac{TP}{TP + FN}$$

Equation 3. Recall Calculation

The statistical analysis of the 2024 Cloud WAF test results indicate the relevance of false positive testing.

8. Contact Information

SecureIQLab, LLC.
9600 Great Hills Trail Suite #150W
Austin, TX 78759 USA
+1.512.575.3457
www.secureiqlab.com
info@secureiqlab.com

9. Copyright and Disclaimer

The content of this report is protected by United States and international copyright laws and treaties. You may only use this report for your personal, non-commercial, informational purposes. Without SecureIQLab's prior written consent, you may not: (i) reproduce, modify, adapt, create derivative works from, publicly perform, publicly display, or distribute this report; or (ii) use this report, the SecureIQLab name, or any SecureIQLab trademark or logo as part of any marketing, promotion, or sales activities. THIS REPORT IS PROVIDED "AS IS," "AS AVAILABLE" AND "WITH ALL FAULTS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, SECUREIQLAB EXPRESSLY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING: (a) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND (b) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF THE REPORT, OR THAT USE OF THE REPORT WILL BE ERROR-FREE, UNINTERRUPTED, FREE FROM OTHER FAILURES OR WILL MEET YOUR REQUIREMENTS. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING SENTENCE, YOU ACKNOWLEDGE AND AGREE THAT THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT DEPEND UPON VARIOUS FACTORS, INCLUDING FACTORS OUTSIDE OF SECUREIQLAB'S CONTROL, SUCH AS: (1) THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF INFORMATION AND MATERIALS PROVIDED BY OTHER PARTIES THAT ARE RELIED UPON BY SECUREIQLAB IN PERFORMING PREPARING THE REPORT; AND (2) THE UNDERLYING ASSUMPTIONS MADE BY SECUREIQLAB IN PREPARING THE REPORT REMAINING TRUE AND ACCURATE. YOU ARE SOLELY RESPONSIBLE FOR INDEPENDENTLY ASSESSING THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT BEFORE TAKING OR OMITTING ANY ACTION BASED UPON THE REPORT. IN NO EVENT WILL SECUREIQLAB BE LIABLE FOR ANY LOST PROFITS OR COST OF COVER, OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING DAMAGES ARISING FROM OR RELATING TO ANY TYPE OR MANNER OF COMMERCIAL, BUSINESS OR FINANCIAL LOSS, EVEN IF SECUREIQLAB HAD ACTUAL OR CONSTRUCTIVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE.

For more information about SecureIQLab and the testing methodologies, please visit our website.

SecureIQLab (May 2024)