SecureIQLab
Independent. Rigorous. Reproducible.
Evidence you can trust.

PUBLIC VALIDATION

# CLOUD WAAP v5.0 CYBERRISK VALIDATION

# COMPARATIVE REPORT


| | |
|---|---|
| **Language:** | English |
| **Report Classification:** | Public Validation |
| **Publication Date:** | August 3, 2026 |

# Table of Contents

# 01
# Executive Summary

SecureIQLab evaluated 12 leading Cloud Web Application and API Protection (WAAP) solutions using the SecureIQLab Cloud WAAP v5.0 CyberRisk Validation Methodology. The assessment measured both Security Efficacy and Operational Efficiency to determine how effectively each solution protects modern web applications and APIs while minimizing operational complexity.

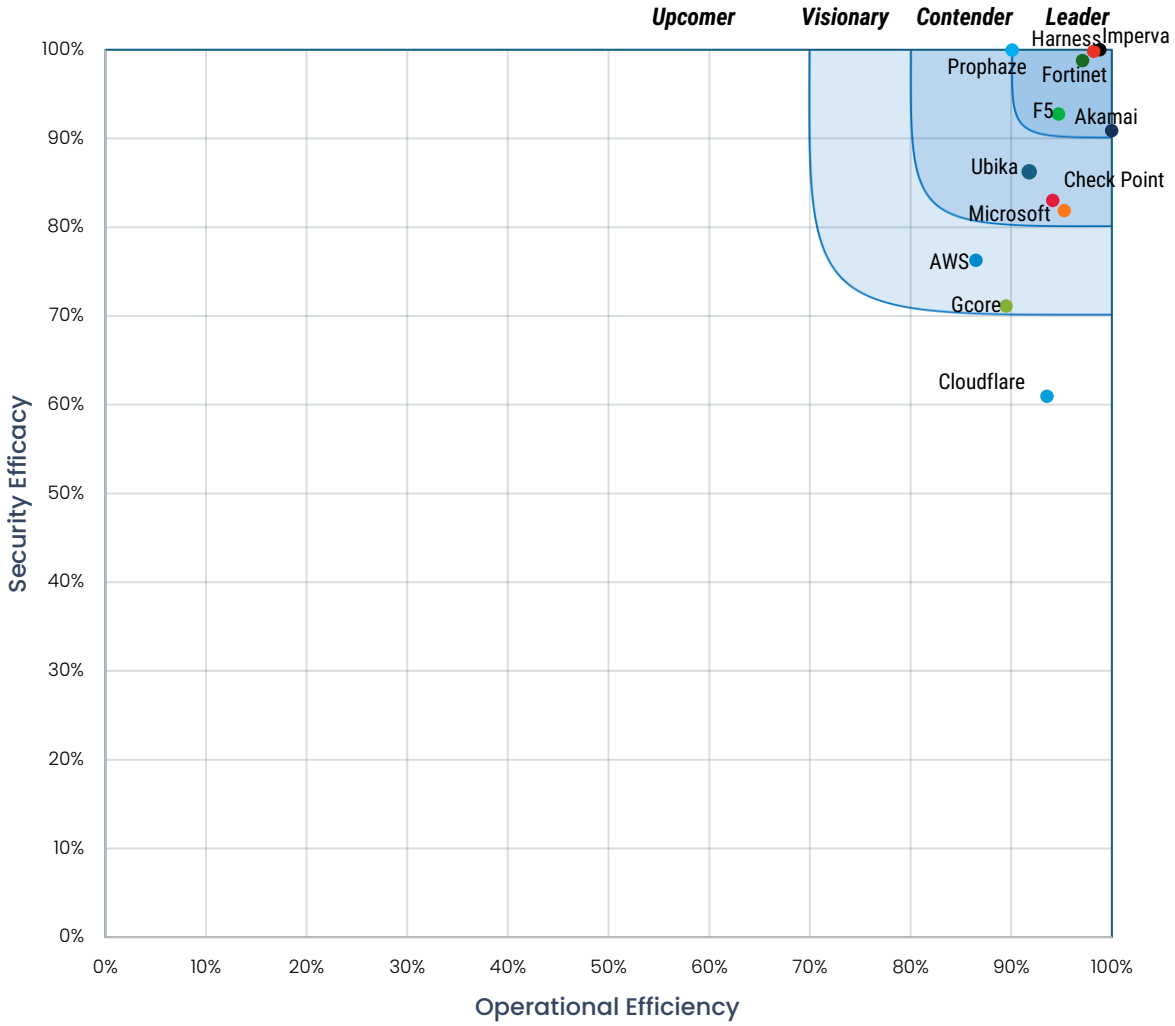


*Figure 1. 2026 Cloud WAAP v5.0 CyberRisk Ripple*

The 2026 Cloud WAAP v5.0 CyberRisk Ripple 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 CyberRisk Methodology v5.0. The higher the security efficacy and operational efficiency scores, the better.

This assessment was conducted using the SecureIQLab Cloud WAAP v5.0 CyberRisk Validation Methodology[1] in accordance with the standards of the Anti-Malware Testing Standards Organization (AMTSO Test ID: AMTSO-LS1-TP169).

This comparative report provides an overview of the results for all tested vendors. The four rankings' vendors fell into are (1) Leader, (2) Contender, (3) Visionary, and (4) Upcomer. In Figure 2, and throughout this report, vendors that completed testing are grouped alphabetically within the applicable ranking. These rankings are derived from the total security efficacy and operational efficiency scores, which are shown in the Cloud WAAP CyberRisk Ripple in Figure 1 on the previous page.

The evaluated Cloud WAAP solutions achieved a group average Complete Security Score of 86.80% and an Operational Efficiency Rating of 94.1%, demonstrating continued market maturity. Six vendors were classified as Leaders, three as Contenders, two as Visionaries, and one as an Upcomer. While overall security efficacy and operational efficiency were strong, the greatest variation was observed in Compliance and OWASP API Security, highlighting areas where vendor capabilities continue to differ.

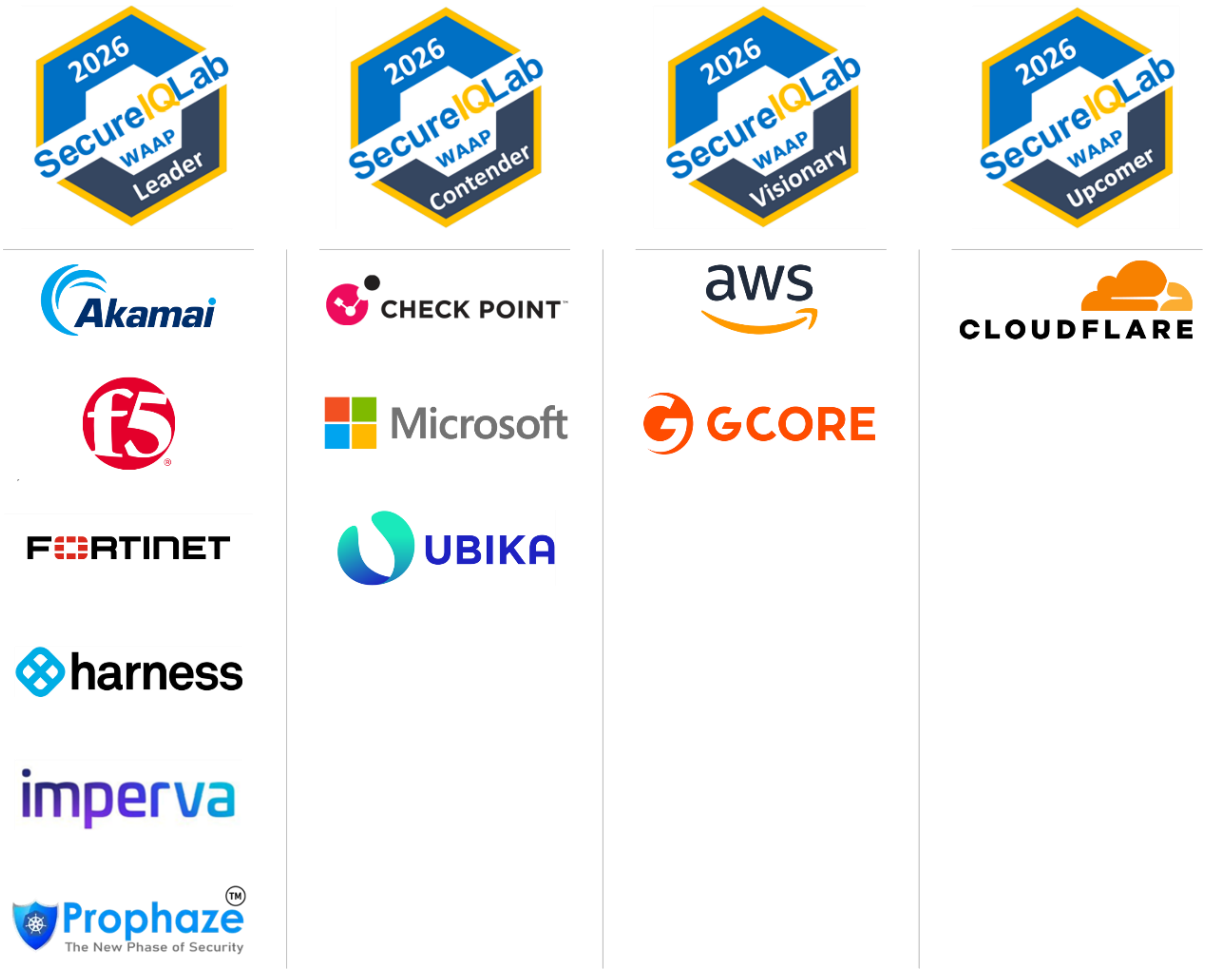


*Figure 2. SecureIQLab WAAP v5.0 Security Vendors*

[1] https://secureiqlab.com/wp-content/uploads/2026/03/Cloud-Web-Application-and-API-Protection-CyberRisk-Methodology-v5.pdf

# 02
# Results Summary

| Vendor | Cloud WAAP Product Name (Deployment Model) | Overall Security Efficacy Score (%) | Overall Operational Efficiency Score (%) | CyberRisk Ripple Category |
|---|---|---|---|---|
| Akamai | App and API Protector (Cloud-based Deployment) | 90.9% | 100% | LEADER |
| AWS | AWS WAF & Amazon CloudFront (AWS Cloud Service) | 76.3% | 86.5% | VISIONARY |
| Check Point | CloudGuard WAF (Cloud based) | 83.0% | 94.2% | CONTENDER |
| Cloudflare | Cloudflare WAF and API Shield (Cloud based) | 60.9% | 93.6% | UPCOMER |
| F5 | F5 Distributed Cloud Web App and API Protection (Cloud based) | 92.7% | 94.7% | LEADER |
| Fortinet | FortiWeb Web Application Firewall v8.0.4 build 95 (GA.M) (AWS AMI) | 98.8% | 97.1% | LEADER |
| Gcore | Gcore WAAP (Cloud based) | 71.1% | 89.5% | VISIONARY |
| Harness | Harness Web Application & API Protection (Cloud-based) | 99.8% | 98.2% | LEADER |
| Imperva | Imperva WAF and API Security (Cloud-based) | 100% | 98.8% | LEADER |
| Microsoft | Azure WAF and API Management (Azure WAF v2) | 81.8% | 95.3% | CONTENDER |
| Prophaze | Prophaze WAAP (Cloud-based) | 99.9% | 90.1% | LEADER |
| Ubika | Ubika WAAP Gateway Cloud v6.16.3 (AWS AMI) | 86.3% | 91.8% | CONTENDER |

*Table 1. SecureIQLab Cloud WAAP v5.0 Results Summary*

Table 1 presents the vendor results in alphabetical order with their overall percentages and their placement category within the SecureIQLab Cloud WAAP v5.0 CyberRisk Ripple.

| Vendor Ranking | Vendors |
|---|---|
| LEADER | Akamai • F5 • Fortinet • Harness • Imperva • Prophaze |
| CONTENDER | Check Point • Microsoft • Ubika |
| VISIONARY | AWS • Gcore |
| UPCOMER | Cloudflare |

*Table 2. WAAP v5.0 vendors ranking*

Table 2 shows that among the 12 validated security solution vendors, Akamai, F5, Fortinet, Harness, Imperva, and Prophaze had exceptional security efficacy & operational efficiency scores in all the primary enterprise categories, placing them in the Leader category, while Check Point, Microsoft and Ubika had above average scores overall placing them in the Contender category. AWS and Gcore had good, compelling solutions, placing them in Visionary, while Cloudflare was placed in the Upcomer due to their below-average overall scores.

Testing included 1,608 attack scenarios, comprising 1,328 web application attacks, 71 API attacks, 174 advanced threat scenarios, 35 OWASP LLM attack scenarios, and 1,487 false-positive scenarios, with normal traffic run on the background throughout the test period. The evaluation was aligned with leading industry frameworks, including the OWASP Top 10 (2025),[2] OWASP API Security Top 10 (2023),[3] OWASP Top 10 for LLM Applications (2025),[4] MITRE ATT&CK,[5] and the Lockheed Martin Cyber Kill Chain,[6] providing comprehensive coverage of modern web application threats, API threats, and AI application threats.

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.[7]

SecureIQLab is dedicated to advancing Cloud WAAP Solutions to ensure they offer the essential protection and operational optimization required in modern cybersecurity environments.

[2] https://owasp.org/Top10/2025/
[3] https://owasp.org/API-Security/editions/2023/en/0x11-t10/
[4] https://genai.owasp.org/llm-top-10/
[5] https://attack.mitre.org/
[6] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html
[7] www.secureiqlab.com/publications/

# 03
# Security Efficacy Comparative

SecureIQLab measured the security efficacy of cloud WAAP solutions by subjecting applications and APIs protected by the products under test to more than 1,600 diverse attack scenarios. The evaluation included validation of OWASP Web Application Security, OWASP API Security, and advanced threat protection capabilities, including Bot Attacks, AI-assisted Bot Attacks, Layer 7 DoS & DDoS attacks, Security Resiliency, and WAAP Vulnerability Assessment. The testing performed by SecureIQLab carries on our tradition of innovation and improvement. During testing, SecureIQLab leveraged SOC$^{X®}$, a proprietary AI-powered cloud security validation platform, to ensure consistency in execution and results.

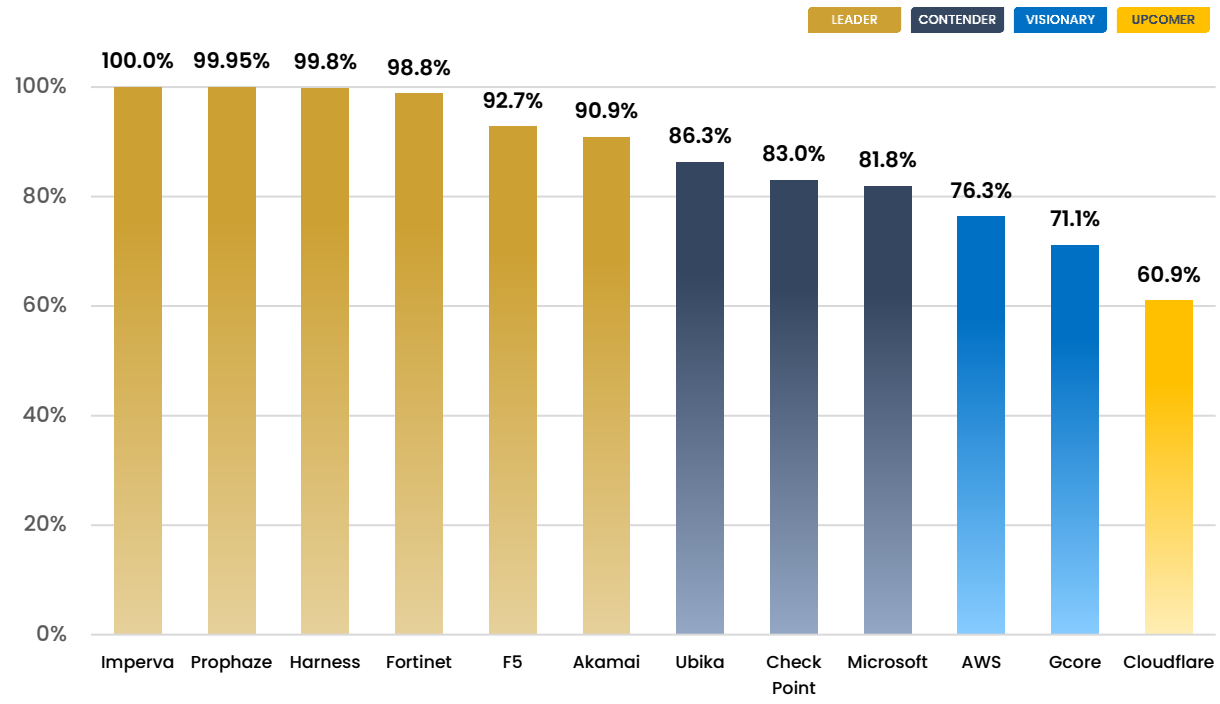


*Figure 3. Security Efficacy Comparative results*

Figure 3 above provides an overview of the SecureIQLab findings during the security validation of the 12 Cloud WAAP solutions. The overall average Complete Security Score is 86.80%, representing an increase of approximately 12.3 percentage points over last year's[8] group average.

[8] https://secureiqlab.com/wp-content/uploads/2025/07/Cloud-WAAP-v4_0_-CyberRisk-Comparative-Validation-Report.pdf

## 3.1 OWASP Web Application Firewall 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 2025.

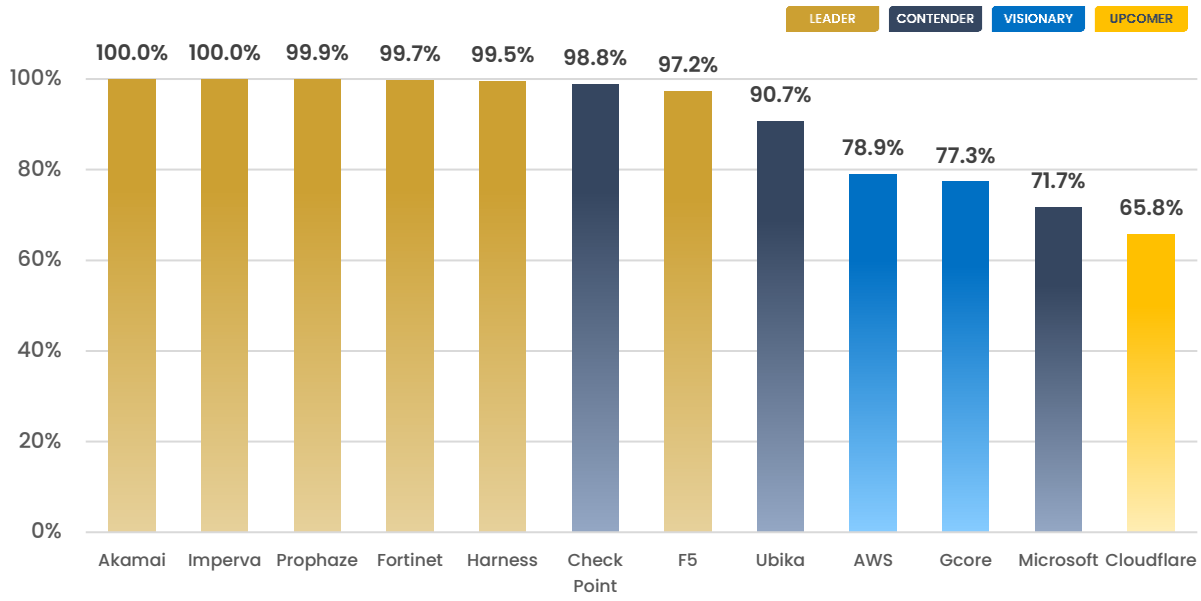


*Figure 4. Overall OWASP WAF Vulnerability Testing*

Figure 4 summarizes the overall OWASP Web Security scores across all 12 Cloud WAAP solutions evaluated in this assessment. Each solution was tested against the OWASP Top 10 Web Application Security vulnerabilities using 34 comprehensive security test categories. The overall group average for OWASP WAF score across the evaluated solutions was 89.96%. For detailed explanations of these attacks, please reference the OWASP Top 10.[9]

[9] https://owasp.org/Top10/2025/

## 3.2 OWASP Application Programming Interface (API) Top 10 Validation

Application Programming Interface (API) security is critical for organizations from a security or regulatory standpoint. An effective WAAP solution must help organizations prevent unauthorized access to sensitive data or functionalities while maintaining reliable operations over multiple protocols. More than 70 attacks were used in the testing of the WAAP solution's API security efficacy. Attacks were selected based on the OWASP API Security Top 10 2023.

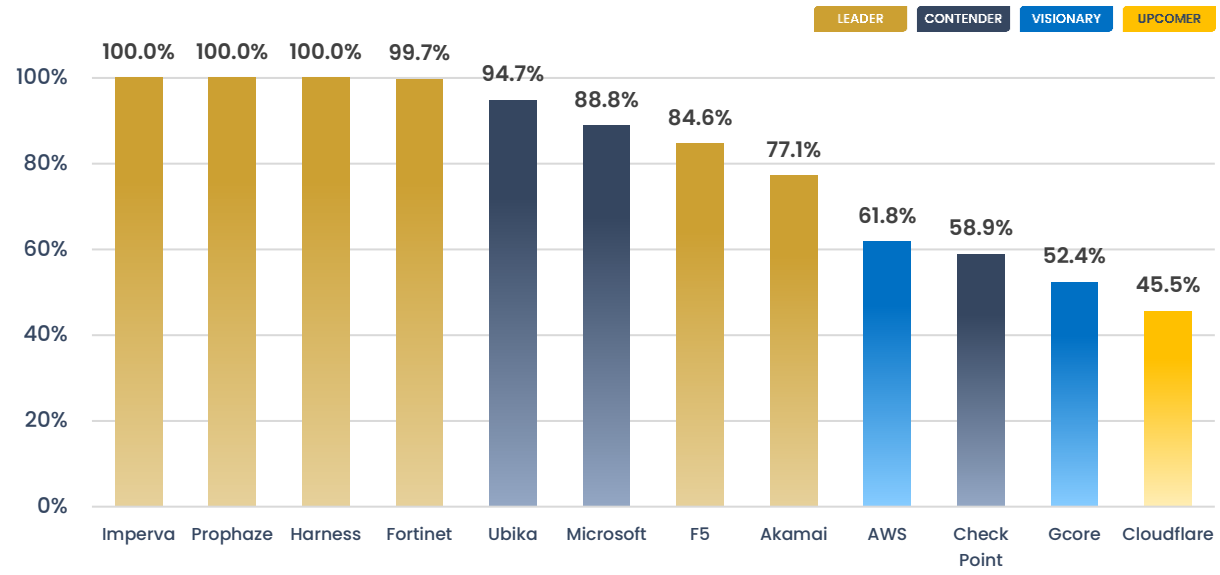


*Figure 5. Overall OWASP API Security Testing*

Figure 5 presents the overall OWASP API Security results across all 12 Cloud WAAP solutions evaluated during the assessment. Each solution was tested against the OWASP API Security Top 10 vulnerabilities using 37 API security test categories. The evaluation covered five widely adopted API protocols, representing the majority of API deployments in modern enterprise environments. The overall group average for OWASP API score across the evaluated solutions was 80.3%. For detailed explanations of these attacks, please reference the OWASP Top 10.[10]

[10] https://owasp.org/API-Security/editions/2023/en/0x11-t10/

## 3.3 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 6 below highlights the combined Bot Attacks, AI-Assisted Bot Attacks, Layer 7 DoS & DDoS Attacks, Resiliency, and WAAP Vulnerability Assessment scores for all 12 vendors.

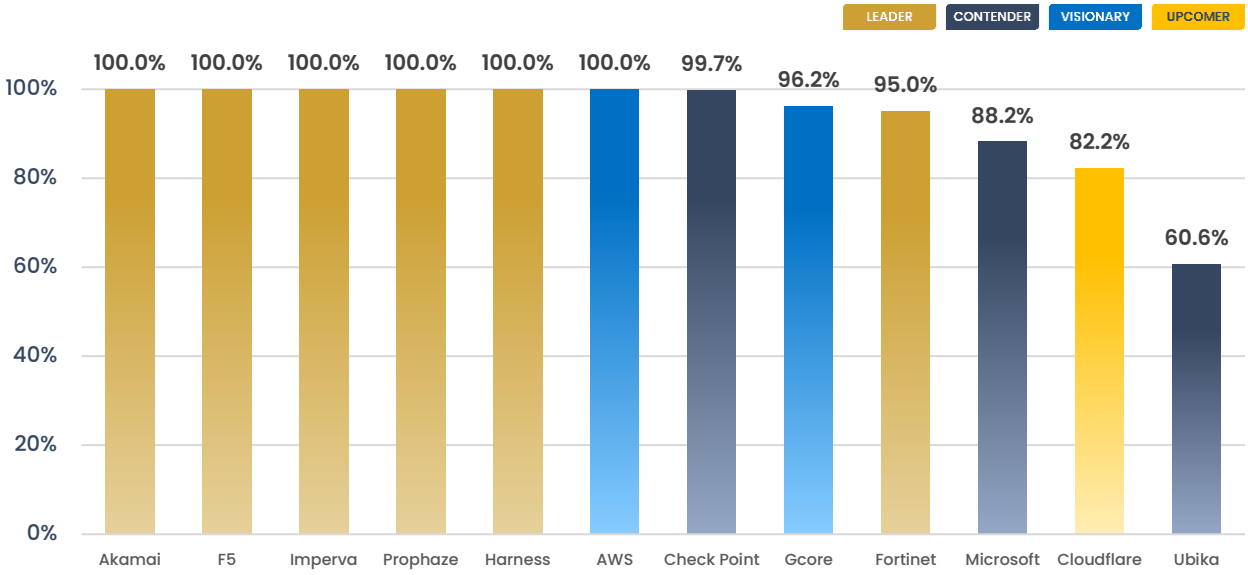


*Figure 6. Overall Advanced Threat Score*

The overall group average for the Advanced Threat score across the evaluated solutions was 93.48%.
For more details on each of the above threat categories, please refer to the cloud WAAP security solutions individual test report published.

# 04
# Operational Efficiency

Operational efficiency in deploying, managing, and utilizing WAAP solutions is critical. SecureIQLab validated WAAP operational efficiency in 9 areas of validation, with a total of 57 features and functions validated. The operational efficiency categories tested were Ease of deployment, Ease of management, Ease of risk management, Logging & Auditing capabilities, Visibility and Analytics, Support and Documentation, API Gateway Efficiency, Integration capabilities and Geolocation-based security features.

Figure 7 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.[11]

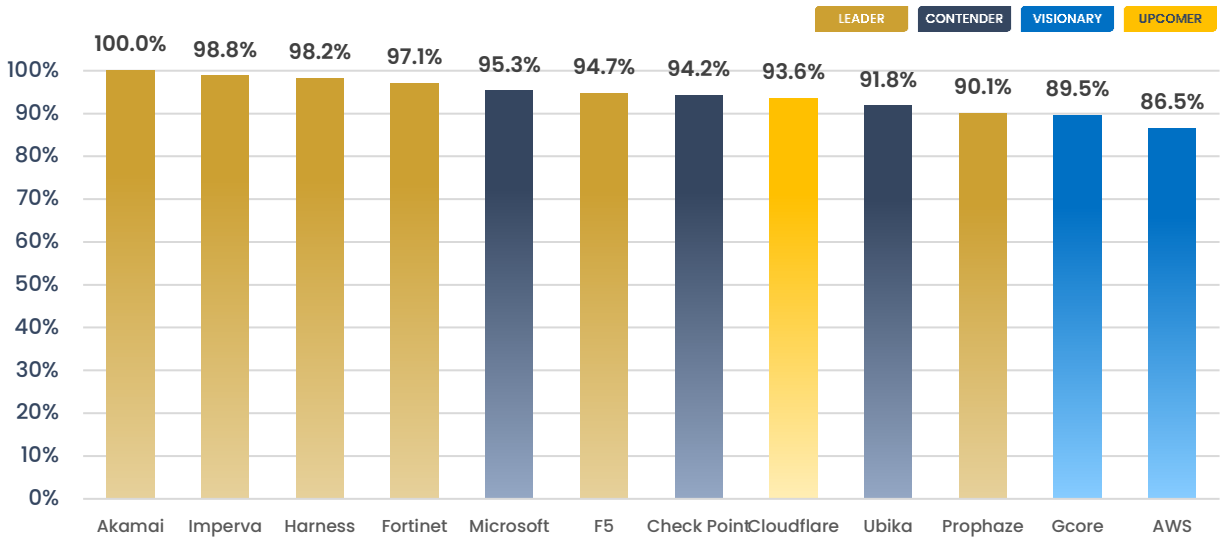


*Figure 7. Overall Operational Efficiency Score*

The overall group average for the Operational Efficiency score across the evaluated solutions was 94.1%. Seven of the twelve evaluated Cloud WAAP solutions achieved Operational Efficiency ratings above the group average, demonstrating strong enterprise operational capabilities across the nine evaluated Operational Efficiency categories.

[11] https://secureiqlab.com/publications/

LEADER CONTENDER VISIONARY UPCOMER

| Operational Efficiency Test Categories | Akamai | AWS | Check Point | Cloudflare | F5 | Fortinet | Gcore | Imperva | Microsoft | Prophaze | Harness | Ubika |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Ease of Deployment | 100.0% | 66.7% | 88.9% | 77.8% | 100.0% | 100.0% | 100.0% | 100.0% | 88.9% | 100.0% | 100.0% | 100.0% |
| Ease of Management | 100.0% | 90.9% | 97.0% | 97.0% | 90.9% | 97.0% | 84.9% | 100.0% | 100.0% | 72.7% | 100.0% | 87.9% |
| Ease of Risk Management | 100.0% | 95.2% | 85.7% | 85.7% | 95.2% | 100.0% | 85.7% | 100.0% | 100.0% | 90.5% | 100.0% | 90.5% |
| Logging & Auditing Capabilities | 100.0% | 85.2% | 100.0% | 88.9% | 92.6% | 100.0% | 85.2% | 100.0% | 88.9% | 96.3% | 96.3% | 92.6% |
| Visibility & Analytics | 100.0% | 93.3% | 100.0% | 100.0% | 100.0% | 100.0% | 93.3% | 100.0% | 100.0% | 93.3% | 100.0% | 93.3% |
| Support & Documentation | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100% | 100.0% | 91.7% | 100.0% | 91.7% |
| API Gateway Efficiency | 100.0% | 80.6% | 94.4% | 94.4% | 100.0% | 100.0% | 88.9% | 94.4% | 100.0% | 100.0% | 97.2% | 88.9% |
| Integration Capabilities | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 100.0% | 66.7% | 100.0% | 100.0% |
| Geolocation-Based Security Features | 100.0% | 55.6% | 66.7% | 100.0% | 66.7% | 55.6% | 88.9% | 100.0% | 55.6% | 100.0% | 88.9% | 100.0% |

*Table 3. SecureIQLab Cloud WAAP v5.0 Operational Efficiency*

### Findings and Observation:

- Support & Documentation and Visibility & Analytics were the most mature operational capabilities, with all evaluated vendors scoring above 90%.
- Geolocation-Based Security Features, Ease of Management, Integration Capabilities, and Ease of Deployment exhibited wide variation among the evaluated solutions, with score ranges of 55.6% to 100%, 72.7% to 100%, 66.7% to 100%, and 66.7% to 100%, respectively.

# 05 AI Application Security and Operational Efficiency

## 5.1 AI Application Security

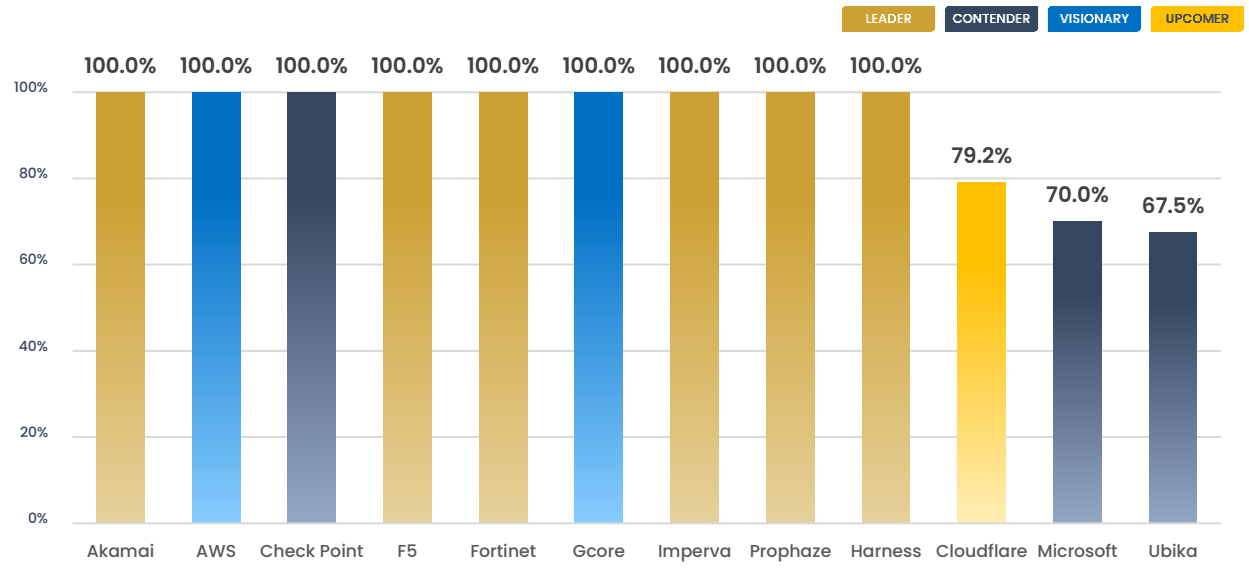


*Figure 8. OWASP Top 10 for LLM Results*

AI-enabled applications introduce new attack surfaces that adversaries can exploit through natural-language interactions with large language models. The OWASP Top 10 for LLM Applications[12] identifies a range of vulnerabilities that arise when generative AI capabilities are integrated into application workflows.

SecureIQLab evaluated 35 attacks targeting AI-enabled applications using techniques aligned with OWASP LLM01 (Prompt Injection) and OWASP LLM05 (Improper Output Handling).

Other risks identified within the OWASP LLM Top 10, such as model training pipeline compromise, model weight theft, model alignment failures, and supply chain risks, primarily involve AI development lifecycle or model governance controls rather than runtime application protections. As a result, these categories were considered outside the scope of WAAP-focused testing.

Figure 8 demonstrates that nine of the 12 evaluated Cloud WAAP solutions achieved a perfect protection score of 100% against the OWASP LLM attack scenarios.

[12] https://genai.owasp.org/llm-top-10/

## 5.2 AI Operational Efficiency

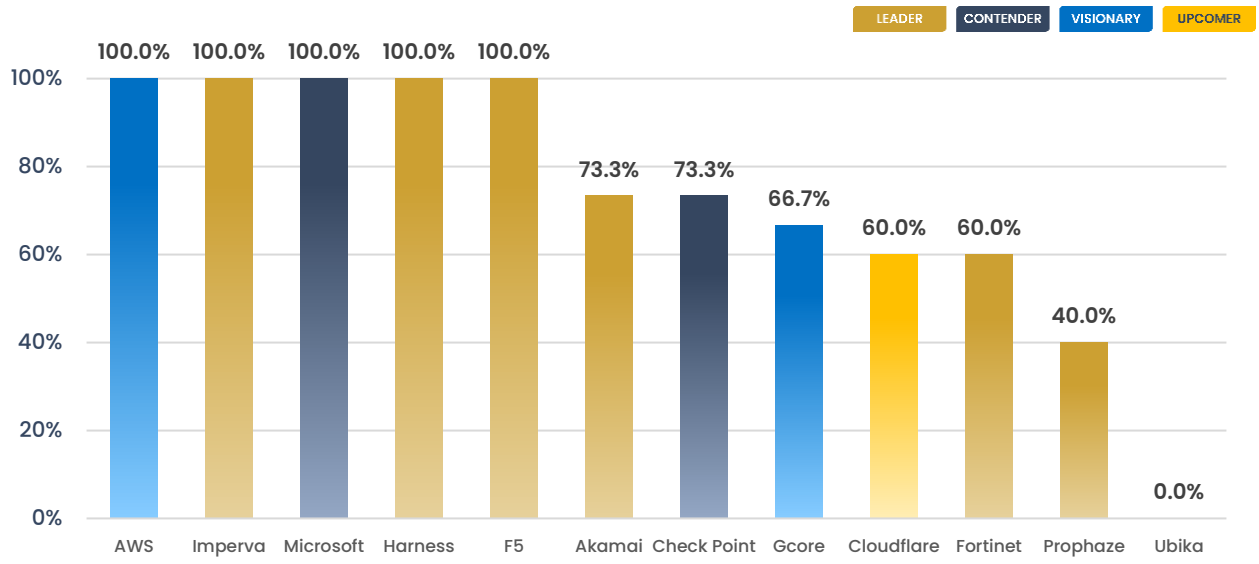


*Figure 9. Operational Efficiency for Gen AI & LLM Results*

SecureIQLab measures the platform's ability to support day-to-day enterprise operations, reduce administrative overhead, and accelerate secure AI adoption. Figure 9 presents the overall Operational Efficiency score for LLM security, reflecting the solution's enterprise readiness to deploy, manage, and govern AI security capabilities.

The OWASP LLM Security Score and the GenAI & LLM Operational Efficiency Rating are evaluated independently and is not factored into the overall Complete Security Score and overall WAAP Operational Efficiency score.

AWS, Imperva, Microsoft, F5 and Harness achieved perfect scores of 100%, demonstrating comprehensive support for enterprise operational capabilities required to deploy, manage, monitor, and secure AI-enabled applications.

# 06 SecureIQLab 'Secure by Design' and 'Secure by Default'

SecureIQLab focused on three core principles that are crucial in evaluating the security posture of WAAP systems during their development lifecycle:

1) Take ownership of customer security outcomes.
2) Embrace radical transparency and accountability.
3) Lead from the top.

SecureIQLab evaluated Secure by Design using three core principles mentioned above, with a total of 22 criteria validated. The highest Secure by Design score achieved in this evaluation was 100%. Vendors that achieved a Secure by Design score of 85% or higher and earned a perfect score of 100% in the WAAP Vulnerability Assessment were awarded SecureIQLab's '*Secure by Design*' badge.


*Figure 10. SecureIQLab's "Secure by Design" Award Winners*

Secure by Default means the product ensures reasonable protection against the most prevalent threats and vulnerabilities without requiring additional configuration from the user. Secure by Default was evaluated using the first two core principles mentioned above, with a total of 13 criteria validated. Vendors that achieved a Secure by Default score of 85% or higher and earned a perfect score of 100% in the WAAP Vulnerability Assessment were awarded SecureIQLab's '*Secure by Default*' badge.


*Figure 11. SecureIQLab's "Secure by Default" Award Winners*

Five of the 12 vendors (AWS, Check Point, F5, Harness, and Microsoft) earned both '*Secure by Design*' and '*Secure by Default*' badges.

# 07
# False Positive Avoidance

Cloud WAAP solutions must accurately distinguish between legitimate user activity and malicious attacks, ensuring that normal business transactions are allowed while threats are blocked. Blocking legitimate user activity can disrupt business operations, increase administrative overhead, and require additional policy tuning.

More than 1,450 false positive test cases were mixed with real-world traffic to validate that the evaluated solutions allowed legitimate user activity while continuing to block malicious requests. These test cases simulated normal user interaction with web applications while being protected by the cloud WAAP.

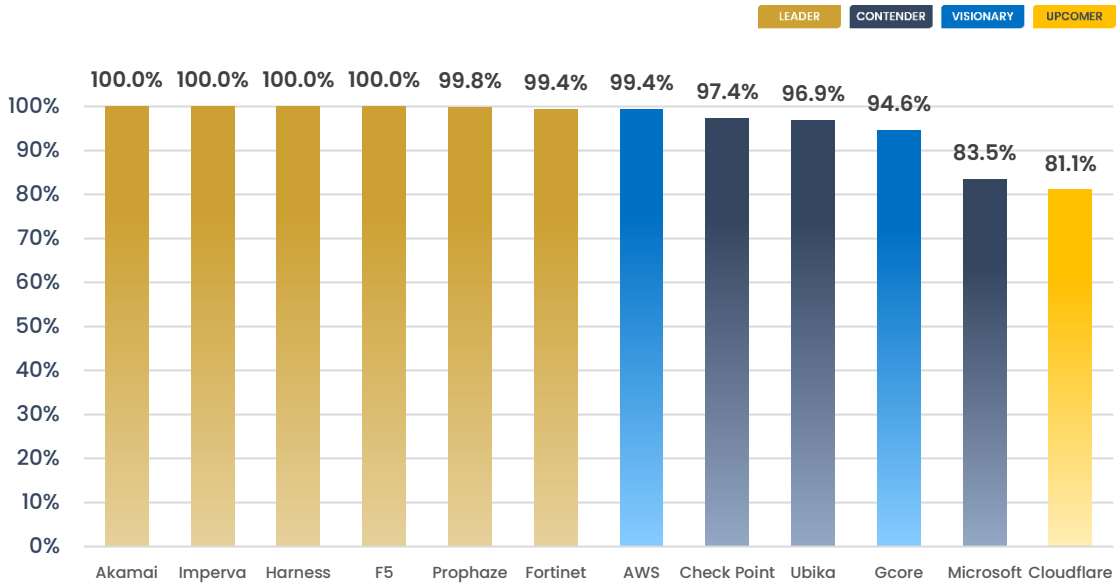


*Figure 12. Overall False Positive Avoidance Score*

False Positive Avoidance scores are the percentage of allowed legitimate activity test cases to the total test cases.

The results for the False Positive Avoidance testing are found in Figure 12. The group average for False Positive Avoidance Score across the evaluated solutions was 96.0%.

# 08
# Compliance

SecureIQLab evaluated compliance by assessing a WAAP solution's ability to satisfy regulatory, data protection, audit, and governance requirements that extend beyond traditional threat prevention. The assessment is derived from internationally recognized cybersecurity and regulatory frameworks, including OWASP Top 10, OWASP API Security Top 10, OWASP Automated Threats, OWASP LLM Top 10, NIST SP 800-53, NIST AI Risk Management Framework (AI RMF), ISO/IEC 27001, ISO/IEC 42001, PCI DSS, GDPR, HIPAA, SOC 2, Developer Security Operations best practices, and global sanctions compliance programs.

The evaluation is organized into five key layers. Together, these layers determine how effectively the solution supports industry regulations, privacy mandates, enterprise governance, and secure application environments.

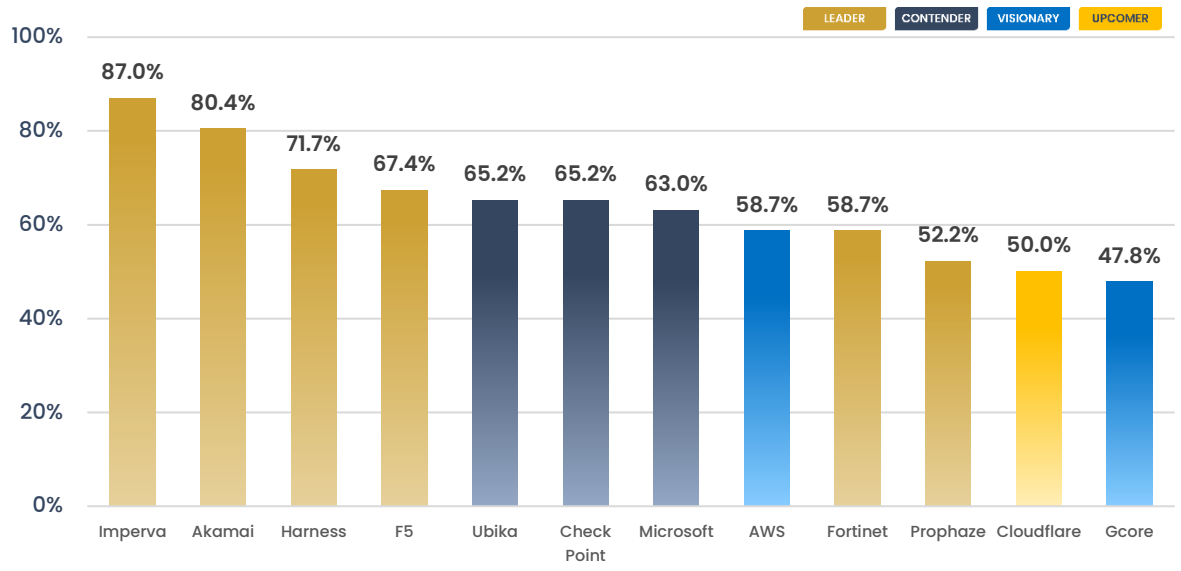


*Figure 13. Compliance Results*

Figure 13 presents the overall Compliance scores for the 12 evaluated Cloud WAAP solutions. The results demonstrate considerable variation in compliance maturity across the evaluated solutions, with scores ranging from 47.8% to 87.0%.

Six out of 12 vendors achieved the score higher than the overall group average of 63.95%.

# 09
# Conclusion

The SecureIQLab Cloud WAAP v5.0 CyberRisk Validation evaluated 12 leading Cloud Web Application and API Protection (WAAP) solutions across multiple categories, including web application security, API security, advanced threat protection, AI application security, operational efficiency, false positive avoidance, Secure by Design, Secure by Default, and compliance. The findings categorize the evaluated Cloud WAAP solutions into 4 distinct tiers based on their combined Security Efficacy and Operational Efficiency within the CyberRisk Ripple.

- **Leaders**: Akamai, F5, Fortinet, Harness, Imperva, and Prophaze emerged as the strongest-performing vendors, consistently achieving high scores across security efficacy and operational efficiency, securing positions in the Leader segment of the CyberRisk Ripple.
- **Contenders:** Check Point, Microsoft, and Ubika were classified as Contenders, demonstrating strong capabilities across both security and operational categories while providing solid enterprise protection.
- **Visionaries:** AWS and Gcore were categorized as Visionaries, offering compelling capabilities with opportunities to further strengthen their overall security and operational maturity.
- **Upcomer:** Cloudflare was placed in the Upcomer category, reflecting opportunities to improve overall security efficacy while maintaining strong operational capabilities.

The group average Complete Security Score of 86.8% and Operational Efficiency score of 94.1% demonstrate that the Cloud WAAP market has matured significantly, with several vendors providing comprehensive protection against modern web application, API, advanced threat, and AI-enabled application attacks. The evaluation also identified greater variability in Compliance and OWASP API Security capabilities across vendors, indicating that these remain key areas for continued product maturity.

Compared with the previous Cloud WAAP v4.0 validation, the group average Complete Security Score increased from 74.51% to 86.80%. Because the vendor cohorts differed between evaluations, this comparison is indicative of overall market progress.

In summary, the evaluation highlights Akamai, F5, Fortinet, Harness, Imperva, and Prophaze as the market leaders, demonstrating the strongest combination of security efficacy and operational excellence. The evaluation further shows that leading Cloud WAAP platforms distinguish themselves through a combination of strong protection, mature operational capabilities, compliance support, and Secure by Design principles as organizations expand AI-enabled applications and API ecosystems.

# 10 Appendix

## Cloud WAAP 2026 Statistical Analysis

At the conclusion of testing, the 2026 Cloud WAAP test results were analyzed statistically. Table 4 presents the Matthews Correlation Coefficient (MCC), Precision, and Recall, which together provide a balanced measure of overall classification accuracy and false positive performance.

| Vendor | MCC | Precision | Recall |
|---|---|---|---|
| Akamai | 0.99 | 1.00 | 0.99 |
| AWS | 0.96 | 0.99 | 0.96 |
| Check Point | 0.94 | 0.98 | 0.97 |
| Cloudflare | 0.57 | 0.81 | 0.75 |
| F5 | 0.97 | 1.00 | 0.97 |
| Fortinet | 0.98 | 0.99 | 0.99 |
| Gcore | 0.86 | 0.95 | 0.91 |
| Harness | 1.00 | 1.00 | 1.00 |
| Imperva | 1.00 | 1.00 | 1.00 |
| Microsoft | 0.66 | 0.84 | 0.83 |
| Prophaze | 1.00 | 1.00 | 1.00 |
| Ubika | 0.86 | 0.96 | 0.90 |
| Average | **0.90** | **0.96** | **0.94** |

*Table 4. Cloud WAAP 2026 Test Statistics*

To better understand these performance metrics, Table 5 provides definitions for the variables used in the calculation of these metrics.

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

*Table 5. Definitions 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 2026 Cloud WAAP test results indicate the relevance of false positive testing.

# 11
# 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 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.

www.secureiqlab.com

COPYRIGHT © 2026 SECUREIQLAB INC. ALL RIGHTS RESERVED.

# About Us

SecureIQLab Inc. is a U.S.-based independent, third-party cybersecurity solution validation and advisory provider. The SecureIQLab security methodology is tailored to what enterprises want, blending research, risk management, and data modeling performed by our deep bench of security experts. SecureIQLab is a member of the Anti-Malware Testing Standards Organization (AMTSO).


**SECUREIQLAB INC.**

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


SecureIQLab
Independent. Rigorous. Reproducible.
Evidence you can trust.