Cloud WAAP v5.0 CyberRisk Comparative Validation

COMMISSIONED REPORT

Akamai Technologies, Inc.
October 26, 2026

SecureIQLab

REPORT DETAILS

Vendor Names:	Akamai, AWS, Cloudflare, F5, Harness, Imperva, Microsoft
Test Dates:	April-July, 2026
Report Classification:	Commissioned Comparative Report
Commissioned by:	Akamai Technologies Inc.

Table of Contents

Cloud WAAP v5.0 CyberRisk Comparative Validation 4

SecureIQLab Cyber Risk Ripple™ 4

01 | Introduction 5

02 | Results Summary 6

03 | Security Efficacy Comparative 8

3.1 | OWASP Web Application Firewall Top 10 Validation 9

3.2 | OWASP Application Programming Interface (API) Top 10 Validation 11

3.2.1 | OWASP API Detection and Prevention Analysis 13

3.2.2 | API Protocol Analysis 17

3.3 | Advanced Threat Coverage 18

3.3.1 | Bot Attacks 18

3.3.2 | AI-Assisted Bot Attacks 19

3.3.3 | Layer 7 DoS Attacks 19

3.3.4 | Security Resiliency Score 20

3.3.5 | WAAP Vulnerability Assessment 20

04 | Operational Efficiency 21

05 | AI Application Security and Operational Efficiency 24

5.1 | AI Application Security 24

5.2 | AI Operational Efficiency 25

06 | False Positive Avoidance 25

07 | Compliance 26

08 | Conclusion 27

09 | Appendix, Copyright, and Disclaimer 28

9.1 | Appendix 28

9.2 | Copyright and Disclaimer 28

10 | About Us 29

Cloud WAAP v5.0 CyberRisk Comparative Validation

COMMISSIONED REPORT

October 26, 2026

SecureIQLab Cyber Risk Ripple™

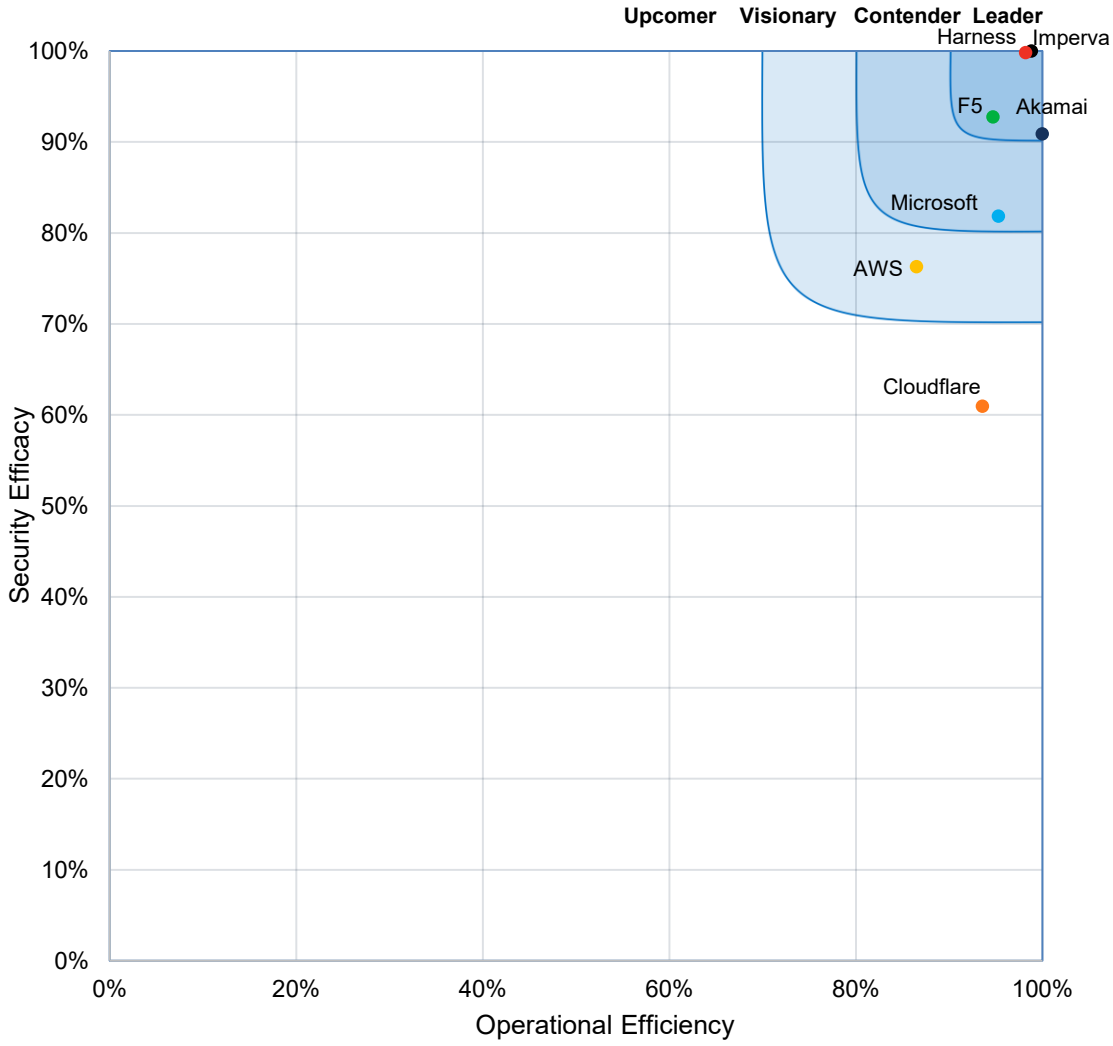


Figure 1. Focused 2026 Cloud WAAP v5.0 CyberRisk Ripple

01 | Introduction

EXECUTIVE SUMMARY

This commissioned comparative report presents findings for seven leading Software as a Service (SaaS) Web Application and API Protection (WAAP) solutions: Akamai Application Protection Platform, comprising App & API Protector and Akamai API Security, AWS WAF & Amazon CloudFront, Microsoft Azure WAF and API Management, Cloudflare WAF and API Shield, F5 Distributed Cloud Web App and API Protection, Imperva WAF and API Security and Harness Application and API Security Platform. The assessment evaluated Security Efficacy and Operational Efficiency to determine how effectively each solution protects modern web applications and APIs while minimizing operational complexity. The comparative findings are limited to the seven solutions included in the scope of this commissioned evaluation.

The Focused 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.

SecureIQLab's focused comparative analysis of seven Cloud WAAP solutions demonstrated strong security performance from Akamai's integrated App & API Protector and API Security solutions. Akamai achieved a 100% OWASP WAF Security Efficacy Score and a 100% Operational Efficiency Score.

Additional analysis of the existing OWASP API Security test data distinguished attacks prevented inline from attacks correctly detected without an inline block. Akamai achieved 95.5% category-averaged overall API threat detection coverage: 58.8% was detected and blocked inline, and an additional 36.7% was detected without an inline block. Akamai achieved 100% detection coverage across the evaluated REST API and GraphQL attack scenarios. Akamai also successfully prevented 100% of the evaluated SOAP and gRPC attacks.

This supplemental analysis provides additional context to Akamai's 77.14% weighted OWASP API Security Efficacy Score by showing how different solution architectures responded through inline prevention versus detection.

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). These seven solutions and their test results are in SecureIQLab's 2026 Cloud WAAP CyberRisk comparative validation report[2].

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 in the background throughout the

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

test period. SecureIQLab validated WAAP operational efficiency in 9 areas of validation, with a total of 57 features and functions validated.

The evaluation was aligned with leading industry frameworks, including the OWASP Top 10 (2025),[3] OWASP API Security Top 10 (2023),[4] OWASP Top 10 for LLM Applications (2025),[5] MITRE ATT&CK,[6] and the Lockheed Martin Cyber Kill Chain,[7] providing comprehensive coverage of modern web application threats, API threats, and AI application threats. The OWASP LLM Security Score and GenAI & LLM Operational Efficiency Rating are evaluated independently and are not factored into the Overall Security Efficacy Score or Overall WAAP Operational Efficiency Score.

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.[8]

This commissioned comparative analysis uses the existing data generated during SecureIQLab's 2026 Cloud WAAP v5.0 CyberRisk Validation. No additional product testing, configuration changes, or retesting were performed for the Detection and Prevention analysis presented in this report. This analysis is intended to provide further context and does not replace or alter the weighted OWASP API Security Efficacy Score used to calculate Overall Security Efficacy.

02 | Results Summary

Vendor	Cloud WAAP Product Name (Deployment Model)	Overall Security Efficacy Score (%)	Overall Operational Efficiency Score (%)
Akamai	**Akamai Application Protection Platform — App & API Protector + Akamai API Security** (Cloud-based)	90.9%	100%
AWS	**AWS WAF & Amazon CloudFront** (AWS Cloud Service)	76.3%	86.5%
Cloudflare	**Cloudflare WAF and API Shield** (Cloud-based)	60.9%	93.6%
F5	**F5 Distributed Cloud Web App and API Protection** (Cloud based)	92.7%	94.7%
Harness	**Harness Web Application & API Protection** (Cloud-based)	99.8%	98.2%
Imperva	**Imperva WAF and API Security** (Cloud-based)	100%	98.8%
Microsoft	**Azure WAF and API Management** (Azure WAF v2)	81.8%	95.3%

Table 1. SecureIQLab Cloud WAAP v5.0 Results Summary

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

Table 1 presents the vendor results in alphabetical order with their overall percentages for Security Efficacy and Operational Efficiency.

Akamai Application Protection Platform achieved an Overall Security Efficacy Score of 90.9% and an Overall Operational Efficiency Score of 100%. Akamai achieved the highest possible Operational Efficiency Score, demonstrating strong performance across the evaluated operational capabilities.

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.

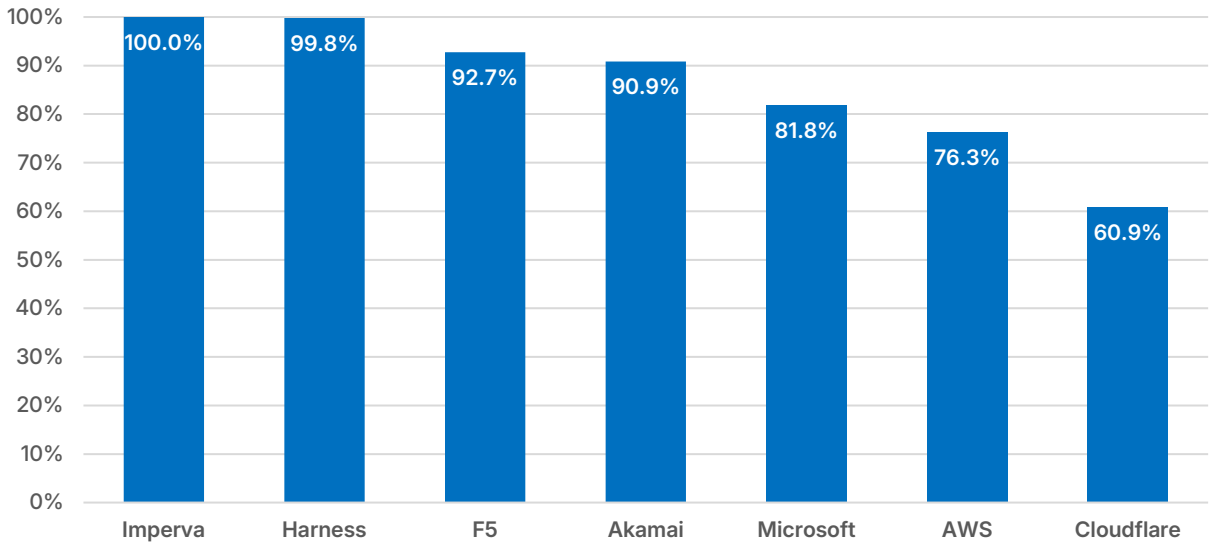


Figure 2. Overall Security Efficacy Score

Figure 2 above provides an overview of the SecureIQLab findings during the security validation of the 7 Cloud WAAP solutions. The Complete Security Score depicts the average of all security categories tested. Equation 1 below depicts the Complete Security Score calculation.

$$\text{Complete Security Score} = \frac{\left(\text{A01 Score} + \ldots + \text{A10 Score} + \text{API1 Score} + \ldots + \text{API10 Score} + \text{Bot Score} + \text{AI Assisted Bot Score} + \text{Layer 7 DoS Score} + \text{Resiliency Score} + \text{Vulnerability Assessment Score}\right)}{25} \times 100\%$$

Equation 1. Calculation of Complete Security Score

Every cloud WAAP evaluated in Complete Security Score was subjected to 25 different test categories with 94 real world-based test sub-categories. The complete security score measures protection against Web Application Firewall specific attacks, API attacks, advanced threat techniques, Bot Attacks, AI-assisted Bot attacks, Layer-7 DoS & DDoS Attacks, Resiliency attacks and WAAP Vulnerability Assessment attacks. SecureIQLab separately evaluated two additional vulnerabilities from OWASP LLM Top 10, which are not included in the Complete Security Score.

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.

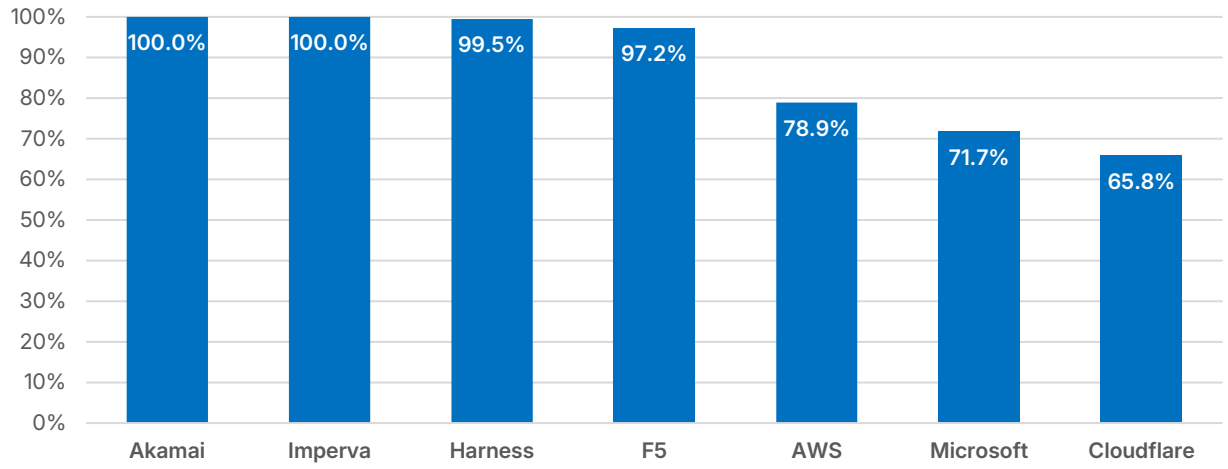


Figure 3. Overall OWASP WAF Vulnerability Testing

Figure 3 summarizes the overall OWASP Web Security scores across all 7 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. For detailed explanations of these attacks, please reference the OWASP Top 10.[9]

The OWASP WAF score is calculated by averaging the ten test categories within the OWASP Top 10 that were validated during testing. Equation 2 below demonstrates the calculation for the OWASP Score.

$$\text{OWASP WAF Score} = \frac{(\text{A01 Score} + \text{A02 Score} + \ldots + \text{A09 Score} + \text{A10 Score})}{10}$$

Equation 2. OWASP WAF Score Calculation

OWASP WAF	Test Case	Akamai % Blocked Score	AWS % Blocked Score	Cloudflare % Blocked Score	F5 % Blocked Score	Harness % Blocked Score	Imperva % Blocked Score	Microsoft % Blocked Score
A01:2025 Broken Access Control	Path Traversal	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	97.7%
	CSRF	100.0%	20.0%	100.0%	100.0%	100.0%	100.0%	0.0%
	SSRF	100.0%	100.0%	73.9%	100.0%	100.0%	100.0%	100.0%
	Unauthorized File Access	100.0%	100.0%	0.0%	100.0%	100.0%	100.0%	33.3%
	Open Redirect	100.0%	100.0%	76.7%	100.0%	100.0%	100.0%	70.0%
	Unrestricted File Upload	100.0%	75.8%	9.1%	100.0%	100.0%	100.0%	45.5%

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

OWASP WAF	Test Case	Akamai % Blocked Score	AWS % Blocked Score	Cloudflare % Blocked Score	F5 % Blocked Score	Harness % Blocked Score	Imperva % Blocked Score	Microsoft % Blocked Score
A02:2025 Security Misconfiguration	XXE	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Tool Based VAPT	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	50.0%
	Geo Fencing Test	100.0%	100.0%	0.0%	100.0%	100.0%	100.0%	0.0%
	Web Cache Poisoning	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
A03:2025 Software Supply Chain Failures	Vulnerable Web Environment	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	80.0%
A04:2025 Cryptographic Failures	JWT	100.0%	96.4%	30.9%	81.8%	100.0%	100.0%	0.0%
A05:2025 Injection	XPath Injection	100.0%	94.4%	22.2%	100.0%	94.4%	100.0%	100.0%
	Host Header Injection	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	SQL Injection	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	OS Command Injection	100.0%	95.0%	35.5%	100.0%	100.0%	100.0%	83.0%
	Cross Site Scripting	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	LDAPI	100.0%	100.0%	3.9%	100.0%	100.0%	100.0%	100.0%
	SSTI	100.0%	96.5%	22.4%	100.0%	100.0%	100.0%	88.2%
	PHP Code Injection	100.0%	98.6%	77.8%	100.0%	100.0%	100.0%	100.0%
A06:2025 Insecure Design	LFI	100.0%	99.0%	93.0%	100.0%	100.0%	100.0%	63.0%
	RFI	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Bot Attacks: Inventory Scraping	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	0.0%
A07:2025 Authentication Failures	Bot Attacks: Login Bruteforce	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Cross Site Scripting XSS	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
A08:2025 Software or Data Integrity Failures	Deserialization Attack	100.0%	0.0%	0.0%	100.0%	100.0%	100.0%	0.0%
A09:2025 Logging and Alerting Failures	Custom Alert Creation	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Alert and Rule Management	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Log Storage Capability	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Auditing Capability	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Log Retention	100.0%	100.0%	33.0%	33.0%	100.0%	100.0%	67.0%
	Granular Security Logging Controls	100.0%	100.0%	100.0%	100.0%	67.0%	100.0%	100.0%
	SIEM/SOAR/S3 Bucket Integration	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
A10:2025 Mishandling of Exceptional Conditions	Improper Error Handling	100.0%	0.0%	0.0%	100.0%	100.0%	100.0%	100.0%

OWASP WAF	Test Case	Akamai % Blocked Score	AWS % Blocked Score	Cloudflare % Blocked Score	F5 % Blocked Score	Harness % Blocked Score	Imperva % Blocked Score	Microsoft % Blocked Score
OWASP WAF SCORE		100.0%	78.88%	65.78%	97.23%	99.51%	100.0%	71.69%

Table 2. OWASP WAF Vulnerability Results

Table 2 presents the OWASP WAF Security Efficacy results across the seven evaluated vendors. Scores ranged from 65.78% to 100%, demonstrating varying levels of protection against the OWASP WAF test cases. Akamai and Imperva demonstrated exceptional performance in the OWASP WAF evaluation, each achieving a 100% in OWASP WAF Security Score.

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. The WAAP solutions were tested against 10 of the OWASP Top 10 API Security vulnerabilities, with 37 test categories validated. More than 70 attacks were used in the testing of the WAAP solution's API security efficacy. API security testing requires fewer attack cases because the assessment focuses on verifying API-specific security controls such as authentication, authorization, schema validation, JWT handling, GraphQL/gRPC protections, rate limiting, and business logic rather than evaluating numerous payload variations. Attacks were selected based on the OWASP API Security Top 10 2023.

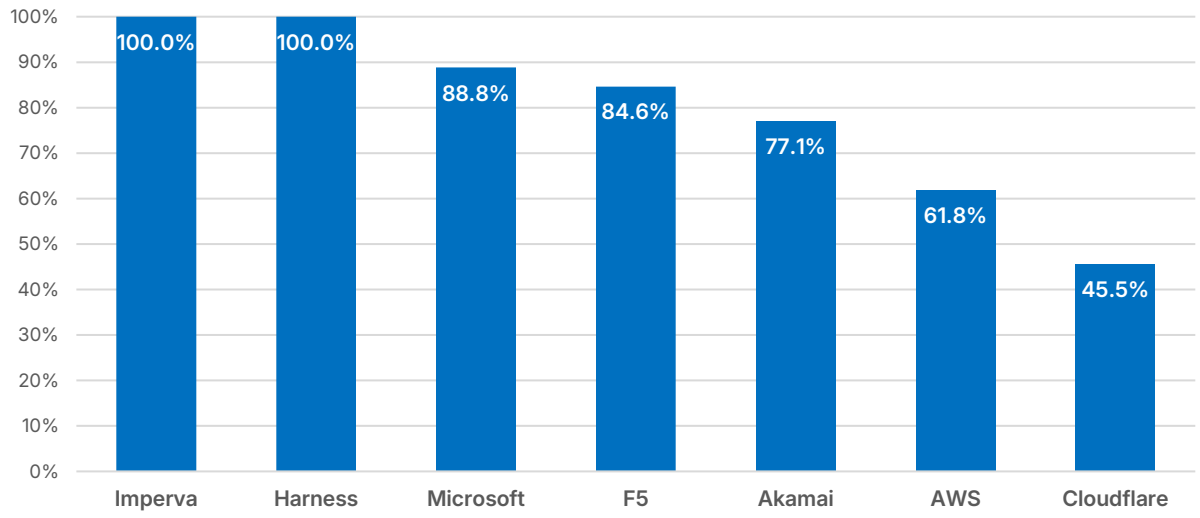


Figure 4. Overall Score for OWASP API Security Top 10 2023 Test Category

Figure 4 illustrates the overall score for OWASP API Security testing across the evaluated WAAP vendors. Scores were provided for prevention as well as detection of the attacks. The scores weighted for inline detection and blocking mitigation are as follows:

- Attack Blocked Inline – 100%
- Attack Detected with Correct Categorization – 50%
- Attack Detected with Incorrect Categorization – 25%
- Attack Allowed – 0%

The OWASP API score is calculated by averaging the ten test categories within the OWASP Top 10. Equation 3 below demonstrates the calculation for the OWASP Score.

$$\text{OWASP API Score} = \frac{(\text{API1 Score} + \text{API2 Score} + \ldots + \text{API9 Score} + \text{API10 Score})}{10}$$

Equation 3. OWASP API Score Calculation

OWASP API	Test Case	Akamai API Score	AWS API Score	Cloudflare API Score	F5 API Score	Harness API Score	Imperva API Score	Microsoft API Score
API1:2023 Broken Object Level Authorization	Horizontal Privilege Escalation (One-Step)	50.0%	0.0%	0.0%	50.0%	100.0%	100.0%	100.0%
	Vertical Privilege Escalation (One-Step)	50.0%	0.0%	0.0%	50.0%	100.0%	100.0%	100.0%
API2:2023 Broken Authentication	Unauthorized Password Change	50.0%	0.0%	0.0%	50.0%	100.0%	100.0%	100.0%
API3:2023 Broken Object Property Level Authorization	Excessive Data Exposure	50.0%	0.0%	0.0%	100.0%	100.0%	100.0%	100.0%
	Mass Assignment	50.0%	100.0%	0.0%	100.0%	100.0%	100.0%	0.0%
API4:2023 Unrestricted Resource Consumption	OTP Rate Limiting	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Aliased based Attack	50.0%	100.0%	0.0%	100.0%	100.0%	100.0%	100.0%
	Deep Recursion Query Attack	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Field Duplication Attack	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Batch Query Attack	50.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Circular Fragment	100.0%	100.0%	0.0%	100.0%	100.0%	100.0%	100.0%
API5:2023 Broken Function Level Authorization	API Endpoint Fuzzing	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	LFI – SOAP	100.0%	100.0%	0.0%	100.0%	100.0%	100.0%	100.0%
	File Creation	100.0%	0.0%	0.0%	100.0%	100.0%	100.0%	100.0%
	Command Injection	100.0%	100.0%	0.0%	100.0%	100.0%	100.0%	100.0%
	Information Disclosure	100.0%	0.0%	0.0%	100.0%	100.0%	100.0%	100.0%
	OSI – WebSocket	0.0%	0.0%	0.0%	0.0%	100.0%	100.0%	0.0%
	LFI – WebSocket	0.0%	0.0%	0.0%	0.0%	100.0%	100.0%	0.0%
API6:2023 Unrestricted Access to Sensitive Business Flows	Large Scale User Registration	100.0%	100.0%	0.0%	100.0%	100.0%	100.0%	100.0%
API7:2023 Server-Side Request Forgery	Server-Side Request Forgery – GraphQL	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Server-Side Request Forgery – RestAPI	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
API8:2023 Security Misconfiguration	Missing CORS	50.0%	100.0%	0.0%	100.0%	100.0%	100.0%	100.0%
	GraphQL Introspection	50.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%

OWASP API	Test Case	Akamai API Score	AWS API Score	Cloudflare API Score	F5 API Score	Harness API Score	Imperva API Score	Microsoft API Score
	GraphQL Field Suggestions	50.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	GraphQL Query Deny List Bypass	50.0%	100.0%	100.0%	100.0%	100.0%	100.0%	0.0%
	Command Execution	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Stored Cross Site Scripting	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	HTML Injection – GraphQL	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	HTML Injection – RestAPI	100.0%	0.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	XSS – REFLECTED	0.0%	0.0%	0.0%	0.0%	100.0%	100.0%	0.0%
	XSS – STORED	0.0%	0.0%	0.0%	0.0%	100.0%	100.0%	0.0%
	XSS – gRPC	100.0%	100.0%	90.0%	0.0%	100.0%	100.0%	0.0%
	XSS – RestAPI	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
API9:2023 Improper Inventory Management	List API Endpoints	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	Discovery of Different API Endpoint Types	100.0%	0.0%	100.0%	100.0%	100.0%	100.0%	100.0%
API10:2023 Unsafe Consumption of APIs	SQL Injection – RestAPI	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
	SQL Injection – GraphQL	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
OWASP API Score		**77.14%**	**61.79%**	**45.51%**	**84.64%**	**100.0%**	**100.0%**	**88.8%**

Table 3. OWASP API Security Vulnerability Testing

Table 3 provides a detailed breakdown of the individual test categories and attack scenarios evaluated within each OWASP API Security Top 10 category. It offers a more granular view of the testing methodology and vendor's performance across the underlying test cases.

3.2.1 | OWASP API Detection and Prevention Analysis

Akamai Application Protection Platform combines distributed inline enforcement through App & API Protector with deeper behavioral and business-logic analysis through Akamai API Security. Some API threats can be identified and blocked from an individual request, while others require broader context across requests, users, sessions, and API activity. API Security performs this deeper contextual analysis outside the request path, and its findings can provide enforcement context to App & API Protector for subsequent matching traffic. This architecture keeps session- and context-intensive analysis outside the request path while maintaining distributed inline enforcement, supporting a performant and resilient API protection strategy.

This commissioned comparative report is based on the existing data from SecureIQLab's 2026 Cloud WAAP v5.0 CyberRisk Validation. The Detection and Prevention analysis presented in this report provides additional insights into the original test results without conducting any new product testing, configuration changes, or retesting. This analysis is intended to provide further context and does not replace or alter the weighted OWASP API Security Efficacy Score used to calculate Overall Security Efficacy.

OWASP API Test Cases	Akamai		AWS		Cloudflare		F5		Harness		Imperva		Microsoft	
	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline
API1:2023	0%	100%	0.0%	0.0%	0.0%	0.0%	0.0%	100%	100%	0.0%	100%	0.0%	100.0%	0.0%
API2:2023	0%	100%	0.0%	0.0%	0.0%	0.0%	0.0%	100%	100%	0.0%	100%	0.0%	100.0%	0.0%
API3:2023	0%	100%	50.0%	0.0%	0.0%	0.0%	100%	0.0%	100%	0.0%	100%	0.0%	50.0%	0.0%
API4:2023	66.7%	33.3%	100.0%	0.0%	66.7%	0.0%	100%	0.0%	100%	0.0%	100%	0.0%	100.0%	0.0%
API5:2023	71.4%	0.0%	42.9%	0.0%	14.3%	0.0%	71.4%	0.0%	100%	0.0%	100%	0.0%	71.4%	0.0%
API6:2023	100.0%	0.0%	100.0%	0.0%	0.0%	0.0%	100%	0.0%	100%	0.0%	100%	0.0%	100.0%	0.0%
API7:2023	100.0%	0.0%	100.0%	0.0%	100.0%	0.0%	100%	0.0%	100%	0.0%	100%	0.0%	100.0%	0.0%
API8:2023	50.0%	33.3%	75.0%	0.0%	74.2%	0.0%	75%	0.0%	100%	0.0%	100%	0.0%	66.7%	0.0%
API9:2023	100.0%	0.0%	50.0%	0.0%	100.0%	0.0%	100%	0.0%	100%	0.0%	100%	0.0%	100.0%	0.0%
API10:2023	100.0%	0.0%	100.0%	0.0%	100.0%	0.0%	100%	0.0%	100%	0.0%	100%	0.0%	100.0%	0.0%
Detection/ Prevention API Scores	58.8%	36.7%	61.8%	0.0%	45.5%	0.0%	74.6%	20%	100%	0.0%	100%	0.0%	88.8%	0.0%

Table 4. OWASP API Security Detection Coverage and Inline Prevention Results

Table 4 presents the OWASP API Security detection coverage results across the seven evaluated solutions, distinguishing between attacks successfully blocked inline and additional attacks detected without blocking. Both components contribute to overall detection coverage, while only inline blocking represents successful prevention.

Vendors	% Blocked Inline	%Detected, Not Blocked Inline	Overall Detection coverage (%)
Akamai	58.8%	36.7%	95.5%
AWS	61.8%	0.0%	61.8%
Cloudflare	45.5%	0.0%	45.5%
F5	74.6%	20.0%	94.6%
Harness	100.0%	0.0%	100.0%
Imperva	100.0%	0.0%	100.0%
Microsoft	88.8%	0.0%	88.8%

Table 5. OWASP API Security Detection Coverage and Inline Prevention Summary

Table 5 presents the overall API threat detection coverage and corresponding inline prevention results across the seven evaluated solutions. Akamai achieved 95.5% category-averaged overall API threat detection coverage: 58.8% was detected and blocked inline, and an additional 36.7% was detected without an inline block.

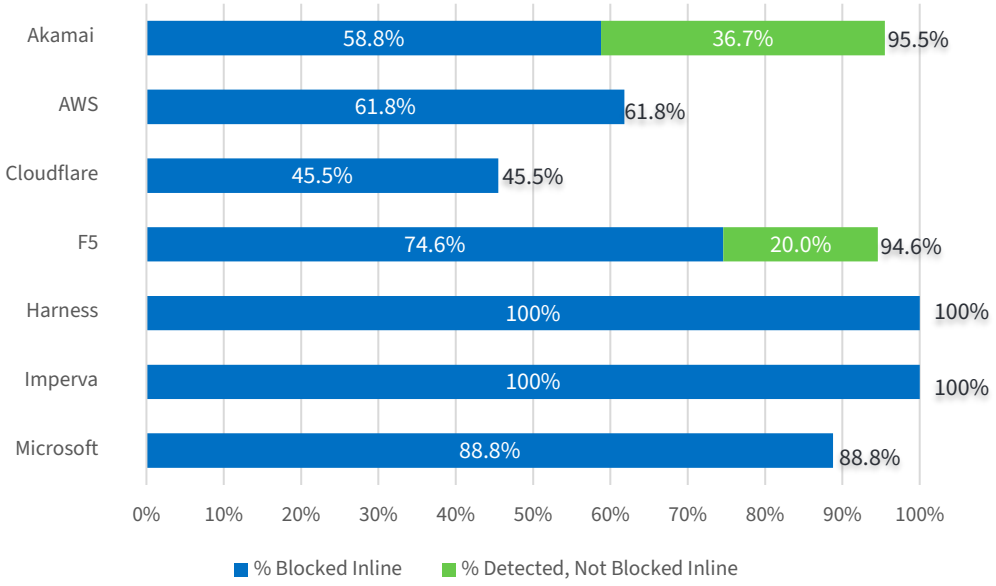


Figure 5. OWASP API Security Detection Coverage and Inline Prevention

Observations

- Akamai achieved 95.5% category-averaged overall API threat detection coverage: 58.8% was detected and blocked inline, and an additional 36.7% was detected without an inline block. Applying the benchmark's weighted scoring criteria, Akamai achieved an OWASP API Security Efficacy Score of 77.14%.
- Akamai detected 100% of the evaluated attacks with correct categorization in API1:2023, API2:2023, and API3:2023, although these attacks were not blocked inline. Akamai prevented 100% of the evaluated attacks in API6:2023, API7:2023, API9:2023, and API10:2023.
- F5 achieved 94.6% category-averaged overall API threat detection coverage: 74.6% was detected and blocked inline, and an additional 20% was detected without an inline block.
- The remaining evaluated solutions received their OWASP API protection credit primarily through inline blocking. Harness and Imperva prevented 100% of the evaluated API attacks, while Microsoft prevented 88.8%, AWS prevented 61.8%, and Cloudflare prevented 45.5%. No additional detection-only coverage was recorded for these five solutions in the summarized results.

OWASP API	Test Case	Akamai % Blocked Inline	Akamai % Detected, Not Blocked Inline
API1:2023 Broken Object Level Authorization	Horizontal Privilege Escalation (One-Step)	0.0%	100.0%
	Vertical Privilege Escalation (One-Step)	0.0%	100.0%
API2:2023 Broken Authentication	Unauthorized Password Change	0.0%	100.0%
API3:2023 Broken Object Property Level Authorization	Excessive Data Exposure	0.0%	100.0%
	Mass Assignment	0.0%	100.0%
API4:2023 Unrestricted Resource Consumption	OTP Rate Limiting	100.0%	0.0%
	Aliased based Attack	0.0%	100.0%
	Deep Recursion Query Attack	100.0%	0.0%
	Field Duplication Attack	100.0%	0.0%
	Batch Query Attack	0.0%	100.0%
	Circular Fragment	100.0%	0.0%
API5:2023 Broken Function Level Authorization	API Endpoint Fuzzing	100.0%	0.0%
	LFI - SOAP	100.0%	0.0%
	File Creation	100.0%	0.0%
	Command Injection	100.0%	0.0%
	Information Disclosure	100.0%	0.0%
	OSI - WebSocket	0.0%	0.0%
	LFI - WebSocket	0.0%	0.0%
API6:2023 Unrestricted Access to Sensitive Business Flows	Large Scale User Registration	100.0%	0.0%
API7:2023 Server-Side Request Forgery	Server-Side Request Forgery – GraphQL	100.0%	0.0%
	Server-Side Request Forgery – RestAPI	100.0%	0.0%
API8:2023 Security Misconfiguration	Missing CORS	0.0%	100.0%
	GraphQL Introspection	0.0%	100.0%
	GraphQL Field Suggestions	0.0%	100.0%
	GraphQL Query Deny List Bypass	0.0%	100.0%
	Command Execution	100.0%	0.0%
	Stored Cross Site Scripting	100.0%	0.0%
	HTML Injection – GraphQL	100.0%	0.0%
	HTML Injection – RestAPI	100.0%	0.0%
	XSS – REFLECTED	0.0%	0.0%
	XSS – STORED	0.0%	0.0%
	XSS – gRPC	100.0%	0.0%
	XSS – RestAPI	100.0%	0.0%
API9:2023 Improper Inventory Management	Ability to List API Endpoints	100.0%	0.0%
	Discovery of Different API Endpoint Types	100.0%	0.0%
API10:2023 Unsafe Consumption of APIs	SQL Injection – RestAPI	100.0%	0.0%
	SQL Injection – GraphQL	100.0%	0.0%
Prevented and Detected API Score for Akamai		**58.8%**	**36.7%**

Table 6. Detailed Breakdown of Akamai's OWASP API Security Inline Prevention and Additional Detection Results

Table 6 provides the detailed breakdown of Akamai's OWASP API Security Results. In the evaluated Akamai Application Protection Platform deployment, edge deployment of the web application protection controls provided inline protection and enforcement, while Akamai API Security contributed behavioral and business-logic detection using broader API activity context. Together, the integrated platform capabilities achieved 95.5% category-averaged overall API threat detection coverage, including 58.8% category-averaged inline prevention.

3.2.2 | API Protocol Analysis

API Security testing was performed over five API protocols: REST-API, GraphQL, SOAP, WebSockets and gRPC. These protocols represent the majority of the API deployments as they exist today. To provide additional context beyond the weighted OWASP API Security Efficacy Score, the results were further analyzed by API protocol and response type i.e. Prevention and Detection.

When the API security results are broken down by protocol, the findings provide additional insight into how each evaluated solution detected and prevented attacks across different API technologies. Table 7 presents the protocol-level OWASP API Security evaluation results, highlighting each vendor's inline prevention and additional detection performance across the five evaluated API protocols.

API Protocols	Akamai		AWS		Cloudflare		F5		Harness		Imperva		Microsoft	
	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline	%Blocked Inline	%Detected, Not Blocked Inline
REST-API	55.6%	44.4%	64%	0.0%	50%	0.0%	78.6%	21.4%	100%	0.0%	100%	0.0%	93%	0.0%
GraphQL	58.7%	41.3%	100%	0.0%	77%	0.0%	100%	0%	100%	0.0%	100%	0.0%	92%	0.0%
SOAP	100%	0%	50.0%	0.0%	0.0%	0.0%	100%	0.0%	100%	0.0%	100%	0.0%	100%	0.0%
WebSockets	0%	0%	0.0%	0.0%	0%	0.0%	0.0%	0.0%	100%	0.0%	100%	0.0%	0%	0.0%
gRPC	100%	0.0%	100%	0.0%	90%	0.0%	0%	0.0%	100%	0.0%	100%	0.0%	0%	0.0%

Table 7. API Security Protocol-Level Prevention and Detection Results

Akamai achieved 100% overall API threat detection coverage for both REST API and GraphQL, through the combination of detection and inline prevention and additional detection without an inline block. Akamai also successfully prevented 100% of the evaluated SOAP and gRPC attacks. WebSocket was the only evaluated API protocol where Akamai demonstrated no protection.

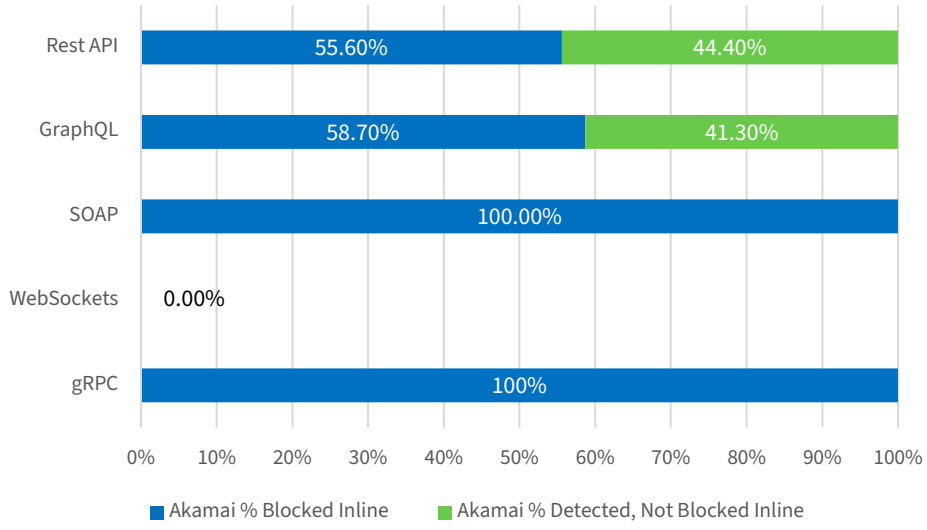


Figure 6. API Protocol-Level Detection Coverage and Inline Prevention

Figure 6 illustrates Akamai's protocol-level inline prevention and additional detection without blocking across the five evaluated API protocols. Akamai achieved 100% overall API threat detection coverage for both REST API and GraphQL, of which 55.6% was detected and blocked inline and an additional 44.4% was detected without inline blocking for REST API, while 58.7% was detected and blocked inline and an additional 41.3% was detected without inline blocking for GraphQL.

Observations

- Akamai, AWS, Microsoft, Cloudflare, and F5 did not demonstrate WebSocket protection in the evaluated test scenarios, resulting in a 0% coverage for that category.
- F5 achieved 100% overall API threat detection coverage for REST API: 78.6% was detected and blocked inline, and an additional 21.4% was detected without an inline block.
- F5 blocked 100% of the evaluated GraphQL and SOAP attacks, while no blocking or detection was observed for evaluated WebSocket or gRPC scenarios.
- Harness and Imperva blocked 100% of the evaluated attacks across all five API protocols: REST API, GraphQL, SOAP, WebSockets, and gRPC.
- AWS blocked 100% of the evaluated GraphQL and gRPC attacks, with blocking rates of 64% for REST API and 50% for SOAP. Microsoft blocked 93% of REST API attacks, 92% of GraphQL attacks, and 100% of SOAP attacks. Cloudflare blocked 50% of REST API attacks, 77% of GraphQL attacks, and 90% of gRPC attacks.

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. This section comprises 174 attack scenarios covering bot attacks, AI-assisted bot attacks, Layer 7 DoS attacks, resiliency testing, and WAAP vulnerability assessments. The tactics and techniques used for these attacks are more important than the volume of the attacks. Tables 8 to 12 below present the combined Bot Attacks, AI-Assisted Bot Attacks, Layer 7 DoS & DDoS Attacks, Resiliency, and WAAP Vulnerability Assessment scores for all 7 vendors.

3.3.1 | Bot Attacks

Bot Attacks	Akamai	AWS	Cloudflare	F5	Harness	Imperva	Microsoft
Large Scale Account Registration	100%	100%	100%	100%	100%	100%	100%
Comment Spamming	100%	100%	100%	100%	100%	100%	100%
User Agent Manipulation	100%	100%	100%	100%	100%	100%	100%
Site Crawling	100%	100%	100%	100%	100%	100%	100%
BOT SCORE	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Table 8. Bot Attack Results

Evaluated WAAP solutions were tested against four advanced types of bot attacks. Bot attacks use automated programs that imitate real users to perform malicious activities, disrupting normal business operations and consuming valuable system resources. The Bot Score is calculated by averaging the four contributing scores.

3.3.2 | AI-Assisted Bot Attacks

AI-Assisted Bot Attacks	Akamai	AWS	Cloudflare	F5	Harness	Imperva	Microsoft
Comment Spamming	100%	100%	100%	100%	100%	100%	100%
Site Crawling	100%	100%	0%	100%	100%	100%	100%
Inventory Scraping	100%	100%	0%	100%	100%	100%	0%
AI-ASSISTED BOT SCORE	**100%**	**100%**	**33%**	**100%**	**100%**	**100%**	**66.7%**

Table 9. AI-Assisted Bot Attack Results

SecureIQLab evaluated the WAAP solution's ability to prevent AI-assisted bot attacks, specifically AI-enhanced comment spamming, site crawling, and inventory scraping. Unlike traditional bot attacks that rely on predefined scripts and predictable behavior, AI-assisted bots leverage generative AI to produce human-like interactions, adapt to defenses, and evade conventional detection techniques.

Table 9 shows the results of the AI-assisted bot attack assessment. Five of the seven vendors achieved a perfect score of 100%, successfully blocking all evaluated AI-assisted bot attack scenarios and outperforming the group average of 86%.

3.3.3 | Layer 7 DoS Attacks

Layer 7 DoS & DDoS	Akamai	AWS	Cloudflare	F5	Harness	Imperva	Microsoft
DDoS - LOIC	100%	100%	100%	100%	100%	100%	100%
Slowhttptest Slow Header (-H)	100%	100%	100%	100%	100%	100%	100%
Slowhttptest Slow Body (-B)	100%	100%	100%	100%	100%	100%	100%
Slowhttptest Slow Read (-X)	100%	100%	100%	100%	100%	100%	100%
Torshammer	100%	100%	100%	100%	100%	100%	100%
MHD DoS	100%	100%	100%	100%	100%	100%	100%
Slowloris	100%	100%	100%	100%	100%	100%	100%
Slowhttptest Apache Killer (-R)	100%	100%	100%	100%	100%	100%	100%
LAYER 7 DoS & DDoS SCORE	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Table 10. Layer 7 DoS & DDoS Results

Layer 7 Distributed Denial-of-Service (DDoS) and Layer 7 Denial-of-Service (DoS) attacks are designed to make web applications slow or unavailable by overwhelming them with website requests that appear to be legitimate user traffic, making them often harder to block than the traditional network flooding attacks. Table 10 presents the results of testing WAAP solutions against one Layer 7 DDoS attack and seven Layer DoS attacks. These attacks map to the MITRE ATT&CK framework, as far as possible.
Each product's *Layer 7 DDoS and DoS Score* was determined by taking the average of its scores against the eight attacks. All seven vendors achieved 100% in eight Layer 7 DoS & DDoS attacks.

3.3.4 | Security Resiliency Score

Resiliency	Akamai	AWS	Cloudflare	F5	Harness	Imperva	Microsoft
XSS	100%	100%	100.0%	100%	100%	100%	100%
OSi – Linux	100%	100%	50.0%	100%	100%	100%	35%
SQLi – User Agent	100%	100%	25.0%	100%	100%	100%	100%
OSi – Windows	100%	100%	44.44%	100%	100%	100%	100%
Path Traversal – Linux	100%	100%	100.0%	100%	100%	100%	100%
Path Traversal – Windows	100%	100%	100.0%	100%	100%	100%	60%
SQLi	100%	100%	100.0%	100%	100%	100%	100%
XSS - Eval	100%	100%	100.0%	100%	100%	100%	0.0%
RESILIENCY SCORE	**100%**	**100%**	**77.43%**	**100%**	**100%**	**100%**	**74.3%**

Table 11. Resiliency Validation Results

Security products must demonstrate resiliency. The prevailing definition of operational resilience is provided by the Department of Defense (DoD), and states it is: "The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions."[10]

Cloud WAAP solutions were tested against 133 resiliency test cases using eight unique attack vectors. These were employed to determine whether it could successfully block attacks that would otherwise go unseen. A higher resiliency score indicates a product is more capable of withstanding and absorbing different variations of attacks, while a lower resiliency score indicates the opposite.

Table 11 presents the resiliency test results across all evaluated test categories. The Resiliency Score represents the average percentage of attacks successfully blocked across the eight resiliency test categories. Akamai, AWS, F5, Harness and Imperva performed notably better than the group average with 100% scores.

3.3.5 | WAAP Vulnerability Assessment

WAAP Vulnerability Assessment	Akamai	AWS	Cloudflare	F5	Harness	Imperva	Microsoft
AppDOS	100%	100%	100%	100%	100%	100%	100%
AccessControl	100%	100%	100%	100%	100%	100%	100%
Authentication	100%	100%	100%	100%	100%	100%	100%
Improper User Authentication	100%	100%	100%	100%	100%	100%	100%
Authentication Session - Management	100%	100%	100%	100%	100%	100%	100%
Configuration Management	100%	100%	100%	100%	100%	100%	100%
Configuration Management - Infrastructure	100%	100%	100%	100%	100%	100%	100%
Configuration Management - Application	100%	100%	100%	100%	100%	100%	100%
Error Handling	100%	100%	100%	100%	100%	100%	100%

[10] https://csrc.nist.gov/glossary/term/operational_resilience

Data Protection	100%	100%	100%	100%	100%	100%	100%
Data Protection - Transport	100%	100%	100%	100%	100%	100%	100%
Input Validation	100%	100%	100%	100%	100%	100%	100%
Input Validation - SQL	100%	100%	100%	100%	100%	100%	100%
Input Validation - OS	100%	100%	100%	100%	100%	100%	100%
Input Validation - LDAP	100%	100%	100%	100%	100%	100%	100%
Input Validation - XSS	100%	100%	100%	100%	100%	100%	100%
Vulnerability Score	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**	**100%**

Table 12. WAAP Vulnerability Assessment Results

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. For that reason, SecureIQLab has assessed the security of the cloud WAAP product itself. All seven WAAP solutions were tested against 16 vulnerability assessment techniques and all of them passed with a 100% score. Table 12 provides the details of our findings.

04 | Operational Efficiency

Operational efficiency in deploying, managing, and utilizing WAAP solutions is critical. SecureIQLab validated WAAP operational efficiency in 9 areas, with a total of 57 features and functions. 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 tested 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.[11]

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

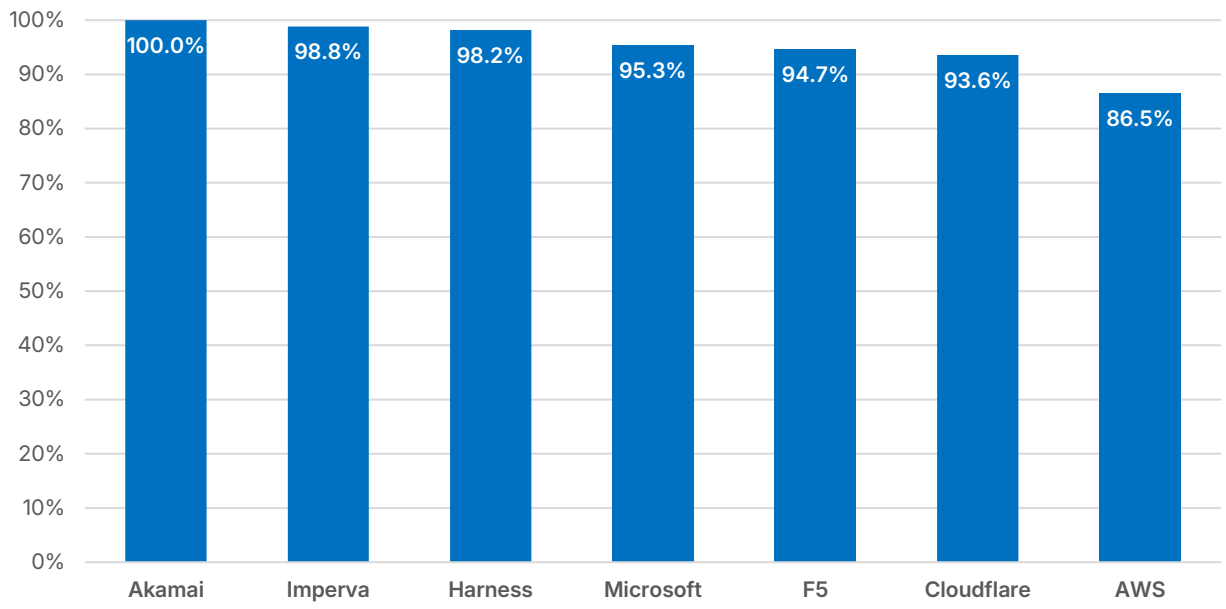


Figure 7. Overall Operational Efficiency Score

Operational Efficiency Test Categories	Akamai	AWS	Cloudflare	F5	Harness	Imperva	Microsoft
Ease of Deployment	100.0%	66.7%	77.8%	100.0%	100.0%	100.0%	88.9%
Ease of Management	100.0%	90.9%	97.0%	90.9%	100.0%	100.0%	100.0%
Ease of Risk Management	100.0%	95.2%	85.7%	95.2%	100.0%	100.0%	100.0%
Logging & Auditing Capabilities	100.0%	85.2%	88.9%	92.6%	96.3%	100.0%	88.9%
Visibility & Analytics	100.0%	93.3%	100.0%	100.0%	100.0%	100.0%	100.0%
Support & Documentation	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
API Gateway Efficiency	100.0%	80.6%	94.4%	100.0%	97.2%	94.4%	100.0%
Integration Capabilities	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%	100.0%
Geolocation-Based Security Features	100.0%	55.6%	100.0%	66.7%	88.9%	100.0%	55.6%

Table 13. SecureIQLab Cloud WAAP v5.0 Operational Efficiency

Table 13 presents the Operational Efficiency results across nine test categories for the seven evaluated WAAP solutions. The evaluation assessed Ease of Deployment, Ease of Management, Ease of Risk Management, Logging & Auditing Capabilities, Visibility & Analytics, Support & Documentation, API Gateway Efficiency, Integration Capabilities, and Geolocation-Based Security Features.

The features and functions within each category are awarded scores based on their capabilities. These scores are then tallied together to form a rating of high, medium, or low. The Operational Efficiency Rating is equal to the total number of WAAP operational efficiency points scored divided by the total number of points possible. Category scores were calculated by aggregating earned points and then dividing this number by the total number of possible points to find a percentage. The average result for each feature validated is used to calculate the test group feature results. Group test averages were then calculated by adding the average score for each feature and then dividing this number by the total number of possible points to find a percentage. Details are available within the individual reports.

Akamai achieved 100% across all nine Operational Efficiency categories, demonstrating consistent results across Deployment, Management, Visibility, API Gateway Operations, Integrations, and Geolocation-Based security capabilities.

05 | AI Application Security and Operational Efficiency

5.1 | AI Application Security

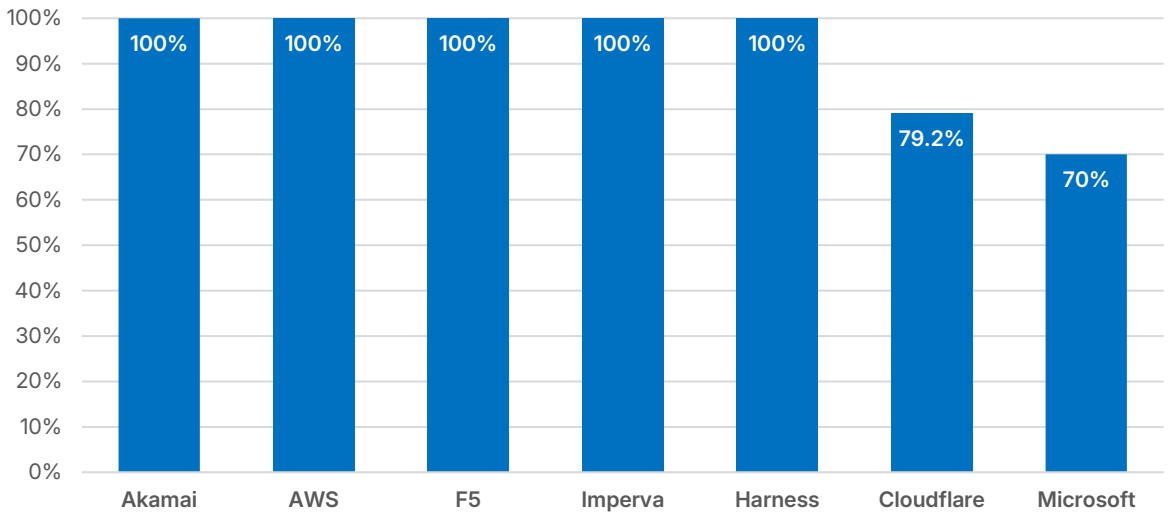


Figure 8. OWASP Top 10 for LLM Results

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 five of the 7 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

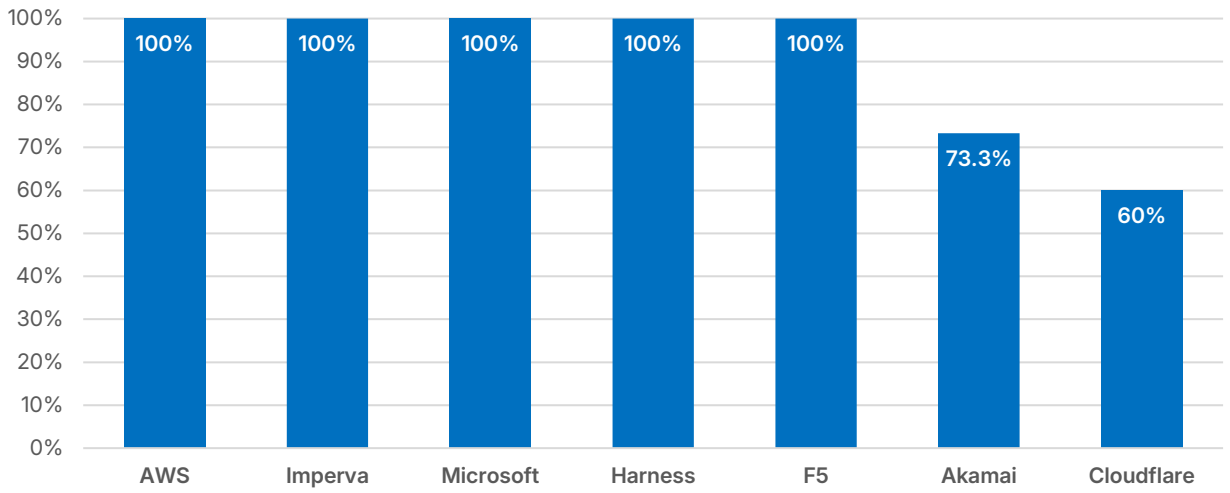


Figure 9. Operational Efficiency for Gen AI & LLM Results

SecureIQLab measured the platforms' 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 solutions' 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 are not factored into the overall Complete Security Score and overall WAAP Operational Efficiency score.

06 | 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.

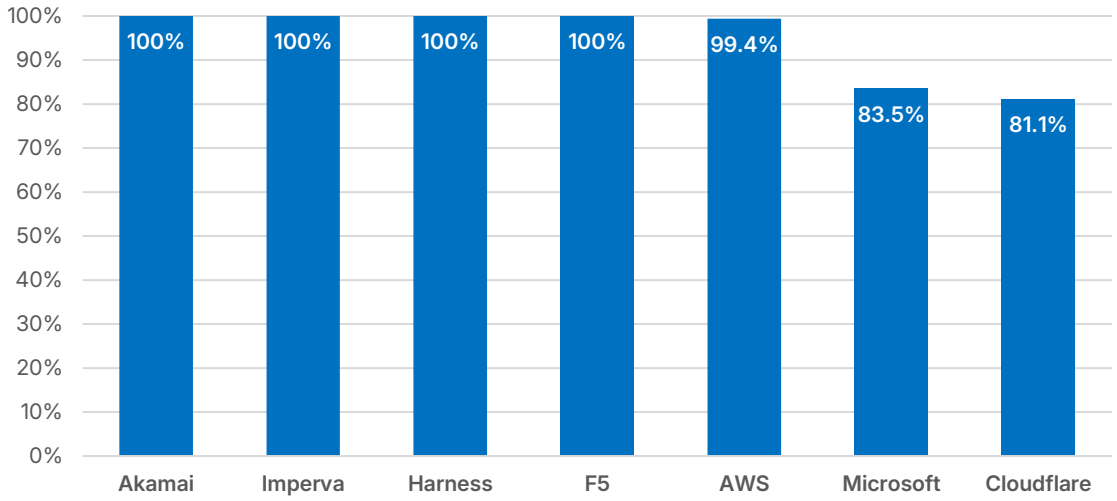


Figure 10. Overall False Positive Avoidance Score

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

The results for the False Positive Avoidance testing are shown in Figure 10. Akamai, Imperva, Harness and F5 achieved a perfect false positive avoidance score of 100%.

07 | 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 11 presents the overall Compliance scores for the 7 evaluated Cloud WAAP solutions. The results demonstrate considerable variation in compliance maturity across the evaluated solutions, with scores ranging from 50% to 87.0%.

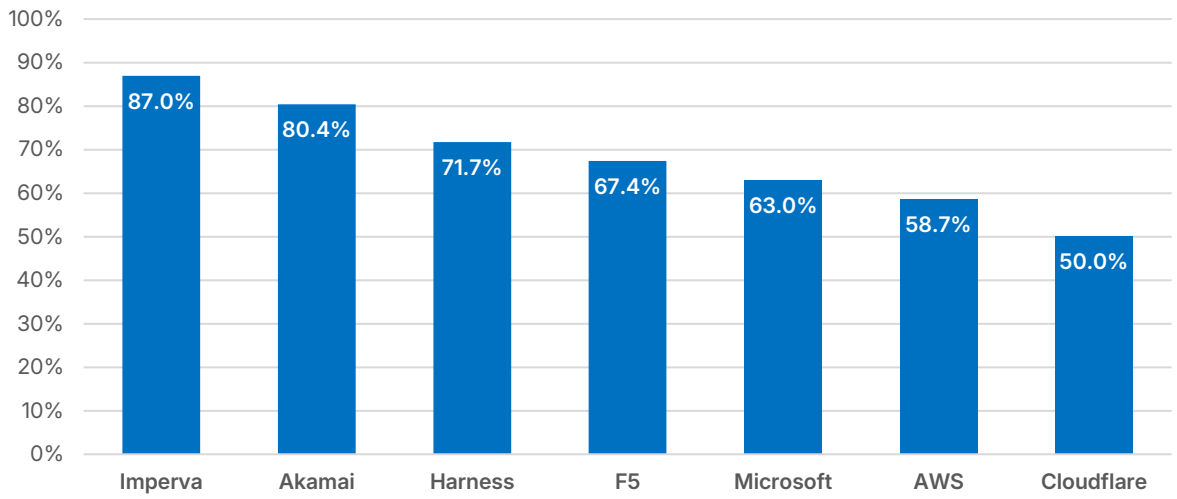


Figure 11. Compliance Results

08 | Conclusion

Akamai Application Protection Platform, comprising App & API Protector and Akamai API Security achieved an Overall Security Efficacy Score of 90.9% and a perfect 100% Overall Operational Efficiency Score, demonstrating strong security performance and consistent operational capabilities across the evaluated categories. Imperva achieved the highest Overall Security Efficacy Score at 100%, followed by Harness at 99.8% and F5 at 92.7%. Microsoft, AWS, and Cloudflare achieved Overall Security Efficacy Scores of 81.8%, 76.3%, and 60.9%, respectively.

Akamai demonstrated particularly strong performance in the OWASP WAF security evaluation, achieving a 100% WAF Security Score. In the OWASP API Security evaluation, Akamai achieved 95.5% category-averaged overall API threat detection coverage: 58.8% was detected and blocked inline, and an additional 36.7% was detected without an inline block. Across the evaluated REST API and GraphQL attack scenarios, Akamai achieved 100% overall API threat detection coverage, through the combination of inline prevention and additional detection-only coverage. Akamai also successfully blocked 100% of the evaluated SOAP and gRPC attacks. WebSocket was the only evaluated protocol where Akamai demonstrated no protection. These results reflect the complementary capabilities of Akamai's integrated App & API Protector and API Security solutions, combining inline enforcement with additional behavioral and business-logic detection. Applying the benchmark's weighted scoring criteria resulted in an OWASP API Security Efficacy Score of 77.14%.

From an operational perspective, Akamai achieved a 100% Operational Efficiency Score and received 100% across all nine evaluated operational categories. Operational results were also high for several of the other evaluated solutions, including Imperva at 98.8%, Harness at 98.2%, Microsoft at 95.3%, F5 at 94.7%, Cloudflare at 93.6%, and AWS at 86.5%.

Akamai, along with Imperva, Harness, and F5, also achieved a perfect 100% False Positive Avoidance Score, demonstrating the ability to accurately distinguish legitimate traffic from malicious activity without incorrectly blocking benign transactions during the evaluation.

Overall, Akamai App and API Protector and API Security solutions demonstrated strong security efficacy, comprehensive operational capabilities, and effective API threat visibility through a combination of inline prevention and additional detection capabilities.

09 | Appendix, Copyright, and Disclaimer

9.1 | Appendix

Please refer to appendix linked **here**.

9.2 | 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. THIS REPORT WAS PREPARED BY SECUREIQLAB AS A COMMISSIONED REPORT. SUBJECT TO THE TERMS OF THE APPLICABLE AGREEMENT WITH SECUREIQLAB, THE COMMISSIONING PARTY MAY REPRODUCE, DISTRIBUTE, PUBLICLY DISPLAY, AND USE THIS REPORT, IN WHOLE OR IN PART, FOR COMMERCIAL, MARKETING, PROMOTIONAL, SALES, AND INFORMATIONAL PURPOSES. SUCH USE MUST NOT MATERIALLY ALTER OR MISREPRESENT THE FINDINGS, RESULTS, OR CONCLUSIONS OF THE REPORT. 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.

10 | 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