SecureIQlab®

Public Test Report

Cloud WAAP CyberRisk Validation Report – Microsoft

Product Version:	**Azure Web Application Firewall and API Security**
Language:	**English**
Published:	**13 May, 2024**

Contents

1. Executive Summary

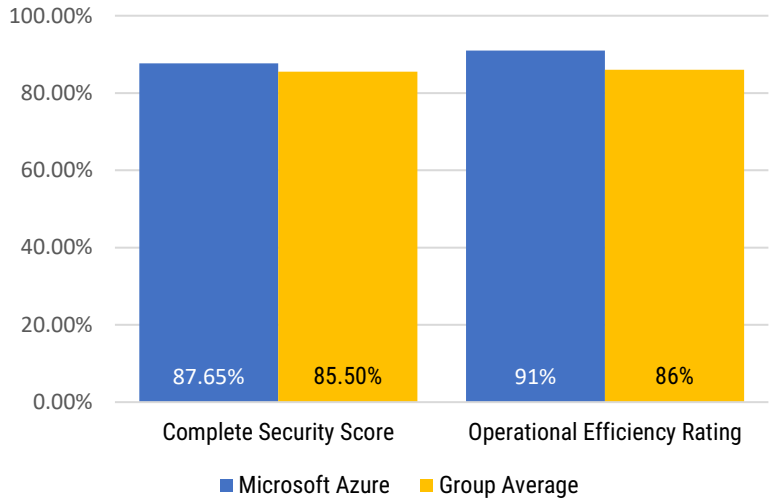


Figure 1. Overall Validation Results for Microsoft Azure WAF and API Security

This report discusses the test results for the Software as a Service (SaaS) Microsoft Azure Web Application Firewall and API Security (WAAP). SecureIQLab completed testing for 12[1] of the leading enterprise-class WAAP solutions to determine their security efficacy and operational efficiency. The higher the security efficacy and operational efficiency scores, the better. The Microsoft Azure Cloud WAAP performed stronger than the group average.

WAAP solutions need to provide outstanding security and control that is easy to implement and efficient to use. This cloud WAAP test evaluated these products' effectiveness in mitigating attacks while minimizing operational burden.

SecureIQLab measured security efficacy for the cloud WAAP solutions by subjecting applications and APIs protected by these products under test to more than 3500 diverse attacks. These attacks were selected based upon industry frameworks such as the OWASP Top 10[2], MITRE ATT&CK, and Lockheed Martin Kill Chain[3]. Roughly 80 features and functions were validated in the evaluation of the WAAPs' operational efficiency. Key operational efficiency validation areas include ease of deployment, management, risk management, scalability, IAM control, visibility & analytics, and logging & auditing capabilities. This comprehensive validation of features and functions further raises the bar in cyber security industry and is unparalleled in contemporary validation and analysis as it exists in the marketplace. Testing was conducted in accordance with the standards of the Anti-Malware Testing Standards Organization[4] (AMTSO). The test used version 3.0 of the SecureIQLab Cloud Web Application Firewall and Application Programming Interface CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP097).

Because thousands of attacks were simulated during the test, test results have necessarily been simplified and presented for review in a summary format. Figure 1 provides a summary of the overall validation results of the Microsoft Azure Web Application Firewall and API Security. Microsoft earned a *Complete Security Score* of 87.65% and an *Operational Efficiency Score* of score of 91%, which are better than the group averages.

This report covers testing for just 1 of the 12 products. An overview comparative report is also available. Reports are also available for the other 11 products tested.

[1] Testing was attempted on a total of 15 cloud WAF solutions. See vendor list for details.
[2] Open Web Application Security Project®.
[3] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.
[4] https://www.amtso.org/

2. Introduction

Cloud-based WAAPs should accurately detect, prevent, and log attack attempts while avoiding false positives. The majority of the attacks conducted against the cloud WAAP product under test were tactics and techniques identified by OWASP for the exploitation of applications and APIs.

Tests were performed utilizing black-box and gray-box testing. Black-box testing assumes that the internal code structure of the product being tested is unknown to the tester. For this testing approach, testers are not required to know a system's implementation details. Gray-box testing assumes that part of the product's internal code structure is known to the tester.

Default configurations and rule sets were used for the majority of the products in this test. However, any "Detect Only" mode settings that were part of default configurations were modified to "Block" mode, with default rulesets used as applicable.

Tuning was based on industry and marketplace expectations that these solutions will require minimal to no tuning during the provisioning, deployment, and management phases. This translates to lower operational expenses and increased revenue for the targeted audience, i.e., SMBs, managed service providers (MSPs), and managed security service providers (MSSPs). To align with the customer experience, any required tuning was performed according to publicly available vendor recommendations.

WAAP-protected applications and APIs were used during testing by performing standard user transactions that included form submissions, comment writing, ecommerce transactions, authentication and authorization, data additional and retrieval, and other transactions. See the Appendix for additional information on the configurations. More detailed information about our testing methods is contained in version 3.0 of the Cloud Web Application Firewall and Application Programming Interface CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP097).

3. Security Efficacy

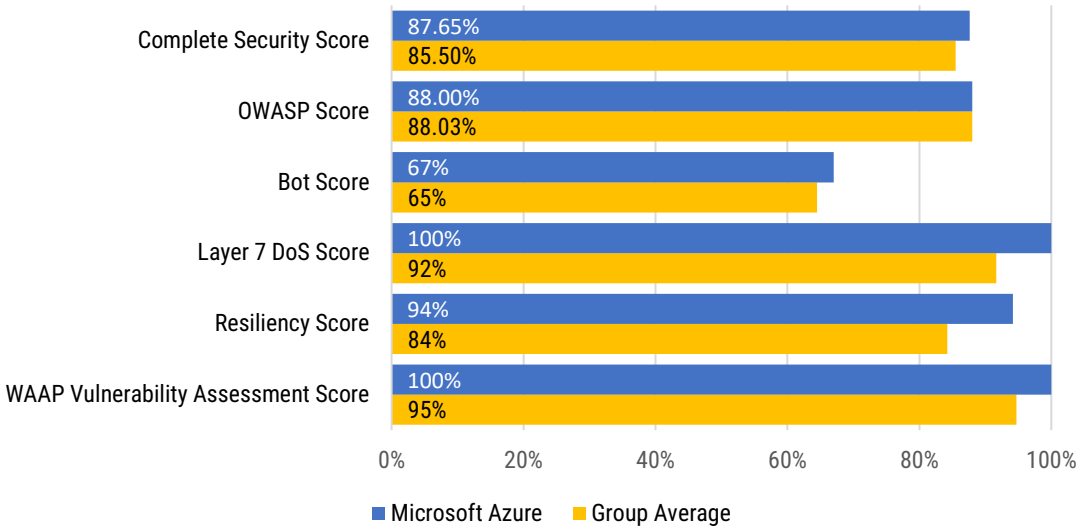


Figure 2. Security Validation Results for Microsoft Azure WAAP

Figure 2 above provides an overview of the SecureIQLab findings during the security validation of the Microsoft Azure WAAP. To summarize, SecureIQLab's testing demonstrates the efficacy of the Microsoft Azure WAAP in this area. The *Complete Security Score* depicts the average of all security categories tested. Equation 1 below depicts the *Complete Security Score* calculation.

$$\text{Complete Security Score} = \frac{\text{A01 Score} + \text{A03 Score} + \text{A04 Score} + \text{A05 Score} + \text{A06 Score} + \text{A07 Score} + \text{A10 Score} + \text{Bot Score} + \text{Layer 7 DoS Score} + \text{Resiliency Score} + \text{WAAP Vulnerability Assesment Score}}{11}$$

Equation 1. Calculation of Complete Security Score

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 alike. Over 3500 validated attacks were used encompassing these scenarios and categories. The testing performed by SecureIQLab carries on our tradition of innovation and improvement. The complete security score consists of Web Application Firewall specific attacks; API attacks were not factored in on this inaugural WAAP test. SecureIQLab will continue to add attack libraries and other relevant operational metrics in future iterations of this test as attacks continue to evolve.

3.1. OWASP Top 10 Validation

The OWASP Top 10[5] lists are assembled by security experts from across the globe and describe the most critical web application and application programming interface vulnerabilities[6]. 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.

3.1.1. OWASP Web Application Firewall Score

OWASP WAF	Test Case	Azure %Blocked/Score	Group Test Average
A01:2021-Broken Access Control	Path Traversal	99.0%	99.5%
	CSRF	0.0%	52.8%
A02:2021-Cryptographic Failures	Cryptographic Failures	100.0%	100.0%
A03:2021-Injection	XPath Injection	96.7%	83.8%
	Host Header Injection	100.0%	88.9%
	HTML Injection	100.0%	94.4%
	SQL Injection (SQLi)	100.0%	98.2%
	OS Command Injection (OSi)	94.1%	73.3%
	Cross Site Scripting (XSS)	100.0%	99.7%
	LDAPi	33.3%	79.5%
	SSTI	80.5%	83.1%
	PHP Code Injection	100.0%	96.9%
A04:2021-Insecure Design	Web Scraping(Parse Hub)	0.0%	50.0%
	LFI	30.5%	71.1%
	RFI	100.0%	87.8%
A05:2021-Security Misconfiguration	Unrestricted File Upload (UFU)	50.0%	82.2%
	XXE	100.0%	83.3%
A06:2021-Vulnerable and Outdated Components	Vulnerable Web Environment	87.5%	88.0%
A07:2021-Identification and Authentication Failures	Bruteforce Attack	100.0%	91.7%
A09:2021-Security Logging and Monitoring Failures	Logging and Monitoring	90.0%	87.1%
A10:2021-Server-Side Request Forgery (SSRF)	SSRF	100.0%	76.4%
OWASP WAF Score		**88.00%**	**88.03%**

Table 1. OWASP WAF Vulnerability Testing

[5] https://owasp.org/www-project-top-ten/

[6] SecureIQLab is not affiliated with OWASP.

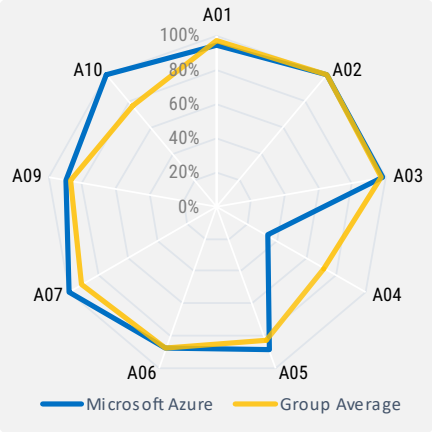


Figure 3. Comparative OWASP WAF Coverage for Microsoft vs Group Average

The Microsoft Azure WAAP was 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 WAAP security. The Figure 3 radar plot shows the relative OWASP coverage area for Microsoft versus the group test average. In the radar plot, more area means better performance.

For detailed explanations of each of these attacks, please reference the OWASP Top 10. Table 1 above provides the results from these tests.

Test case averages are calculated by determining the percentage of the total attacks blocked to the total attacks used in the test case. Category averages are determined by calculating the percentage of the total number of blocked attacks divided by the total number of attacks for all the test cases within each category. As an example, Equation 2 below provides the formula for calculating the average for the *A01 Broken Access Control* vulnerabilities category.

$$A01\ Broken\ Access\ Control = \frac{Total\ \#\ CSRF\ Attacks\ Blocked + Total\ \#\ Path\ Traversal\ Attacks\ Blocked}{Total\ \#\ CSRF\ Attacks + Total\ \#\ Path\ Traversal\ Attacks} \times 100\%$$

Equation 2. Formula for Calculating the Average for A01 Broken Access Control Vulnerabilities OWASP Category

The OWASP score is calculated by averaging the nine test categories within the OWASP top 10 that were validated during testing. Equation 3 below demonstrates the calculation for the OWASP Score.

$$OWASP\ Score = \frac{A01\ Score + A02\ Score + A03\ Score + A04\ Score + A05\ Score + A06\ Score + A07\ Score + A09\ Score + A10\ Score}{9}$$

Equation 3. OWASP Score Calculation

Please see the Appendix for information regarding mapping the OWASP test cases to the MITRE ATT&CK Enterprise Framework.[7]

From the above, Microsoft demonstrated superior security coverage over 8 of the 9 OWASP categories tested. Microsoft scored 100% in 10 out of the 21 validated test cases and scored on par with the group average.

3.1.2. OWASP Application Programming Interface Security Rating

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.

This inaugural test of API Security was executed to understand the current state of API security as it exists in the marketplace. No relevant dataset exists, and these API security results serve as a baseline of the WAAP industry. Security Testing was performed over six API protocols. These protocols represent the majority of the API deployment as it exists today. More than 70 attacks were used in the testing of the WAAP's API Security efficacy. Attacks were selected based on the OWASP API Security Top 10 2023.

[7] SecureIQLab is not affiliated with The MITRE Corporation.

OWASP API	Azure Rating (1-5)	Group Average (1-5)
API1:2023 - Broken Object Level Authorization	1	2.7
API2:2023 - Broken Authentication	1	2.3
API3:2023 - Broken Object Property Level Authorization	1	2.8
API4:2023 - Unrestricted Resource Consumption	4	2.7
API5:2023 - Broken Function Level Authorization	2	2.3
API6:2023 - Unrestricted Access to Sensitive Business Flows	1	3.7
API7:2023 - Server Side Request Forgery	5	2.3
API8:2023 - Security Misconfiguration	1	2.0
API9:2023 - Improper Inventory Management	1	2.8
API10:2023 - Unsafe Consumption of APIs	5	5.0
OWASP API Rating	**2.2**	**2.9**

Table 2. OWASP API Security Rating Results

Protocols Tested	Azure Rating (1-5)	Group Average (1-5)
REST-API	2	3.2
GraphQL	4	3.2
SOAP	3	3.4
Kubernetes	5	3.5
WebSockets	1	1.9
gRPC	1	2.3
API Security Rating	**2.7**	**2.9**

Table 3. API Security Results for Tested Protocols[8]

Table 2 highlights the results of testing against the OWASP API framework. Table 3 highlights the results from this testing for the API Security Rating for each protocol tested. Ratings are between 1 and 5 where 5 represents the highest security efficacy. The rating system is as follows:

Rating of 5: Security Efficacy ≥ 90%
Rating of 4: 90% > Security Efficacy ≥ 70%
Rating of 3: 70% > Security Efficacy ≥ 45%
Rating of 2: 45% > Security Efficacy ≥ 20%
Rating of 1: 20% > Security Efficacy

The above data showcases Microsoft's OWASP API Security protection and almost average security coverage over various protocols. Currently, API security testing is not part of the *Complete Security Score*. Future iterations of this test will see the results included in the *Complete Security Score*.

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. This section consists of Bot Attacks, Layer 7 DoS Attacks, Resiliency, and WAAP Vulnerability assessment.

[8] The Microsoft Azure API Management (APIM) solution, not tested in this iteration, may provide additional advanced API security capabilities and features when integrated with the Microsoft Azure WAF and API Security solution.

3.2.1. Bot Attacks

For purposes of this test, a bot is defined as an automated tool that is used by a remote attacker to carry out automated attacks. The bot tool can exist on the attacker's computer or a compromised endpoint. The Microsoft Azure WAAP was tested against five types of bot attacks. Two of these bot attacks are part of the OWASP security validation. The remaining three attacks are scored within this category. These attacks were initiated from Asian and North American locations to determine whether the geolocation of an attack source impacts the product's security effectiveness. Results show that geolocation does not impact the product's security effectiveness. The *Bot Score* is calculated by averaging the three contributing scores. The maximum *Bot Attack Score* for the tested vendors was 100%. The minimum *Bot Attack Score* for the tested vendors was 0%.

Bot Attacks	Azure Results	Group Average
Web Crawler	Blocked	67%
Broken Link Checker	Blocked	67%
User Agent Manipulation	Contact SecureIQLab	50%
Bot Score	**67%**	**65%**

Table 4. Bot Attack Results

Table 4 shows Microsoft missed one bot attack and performed slightly better than the group average.

3.2.2. Layer 7 DoS Attacks

Layer 7 Distributed Denial-of-Service (DDoS) and Layer 7 Denial-of-Service (DoS) attacks are more difficult to detect than other DDoS and DoS layer attacks because they use a valid TCP connection. Below, Table 5 presents the results of testing Microsoft's Azure WAAP against two Layer 7 DDoS attacks and five Layer DoS attacks. These attacks to the MITRE ATT&CK framework, as far as possible. The product's *Layer 7 DDoS and DoS Score* was determined by taking the average of its scores against the seven attacks. The highest Layer 7 DDoS Score of the group of tested vendors in this category was 100%, and the lowest rating was 57%.

Layer 7 DoS	Azure Results	Group Average
DDoS - LOIC	Blocked	83%
Slowhttptest Slow Header (-H)	Blocked	92%
Slowhttptest Slow Body (-B)	Blocked	83%
Slowhttptest Slow Read (-X)	Blocked	100%
Torshammer	Blocked	92%
MHDDoS	Blocked	92%
Slowloris	Blocked	100%
Layer 7 Dos Score	**100%**	**92%**

Table 5. Layer 7 DoS Results

Microsoft blocked both Layer 7 DDoS attacks and all five of the Layer 7 DDoS attacks, earning a perfect score.

3.2.3. Resiliency Score

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."[9]

To test its operational resilience, The Microsoft Azure WAAP was tested against 103 resiliency test cases using 3 unique attack vectors, which 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 6 below provides the Microsoft Azure Web Application Firewall and API Security results for the test cases. The *Resiliency Score* is the percentage of attacks blocked out of the total 103 attacks. The maximum *Resiliency Score* for the tested vendors was 99.3% and the minimum *Resiliency Score* for the tested vendors was 54.9%.

Resiliency	Azure Results	Group Average
Cross Site Scripting	83%	89%
OS Command Injection	100%	73%
SQL Injection	100%	92%
Resiliency Score	**94.2%**	**84.3%**

Table 6. Resiliency Validation Results

Microsoft performed notably better than the group average *Resiliency Score*.

3.2.4. WAAP Vulnerability Assessment

WAAP Vulnerability Assesment	Azure Results	Group Average
Configuration & Deployment Management	Pass	92%
Identity Management Testing	Pass	100%
Authentication Testing	Pass	92%
Authorization Testing	Pass	92%
Session Management Testing	Pass	92%
Input Validation Testing	Pass	92%
Testing for Error Handling	Pass	100%
Testing for Weak Cryptography	Pass	100%
Business Logic Testing	Pass	100%
Client-side Testing	Pass	83%
API Security testing	Pass	100%
WAAP Vulnerability Assessment Score	**100%**	**95%**

Table 7. 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. SecureIQLab has assessed the security of the cloud WAAP product itself.

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

Microsoft was tested against 11 vulnerability assessment techniques that are commonly used to assess the hardness of WAAP systems. Furthermore, this assessment also represents secure design outcomes. Table 7 provides the details of our findings. Seven out of the 12 WAAP solutions tested passed the WAAP Vulnerability Assessment with a score of 100%.

Microsoft performed better than average in the WAAP vulnerability assessment and earned a perfect score. For earning a 100% WAAP Vulnerability Assessment Score, SecureIQLab rates Microsoft as "Secure by Design".

4. Operational Efficiency

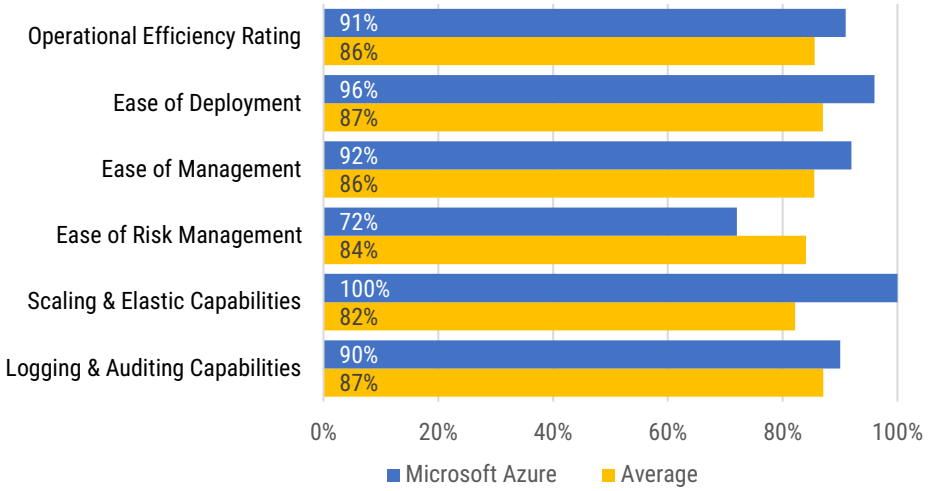


Figure 4. Overview of Operational Efficiency Results for Microsoft Azure Web Application Firewall

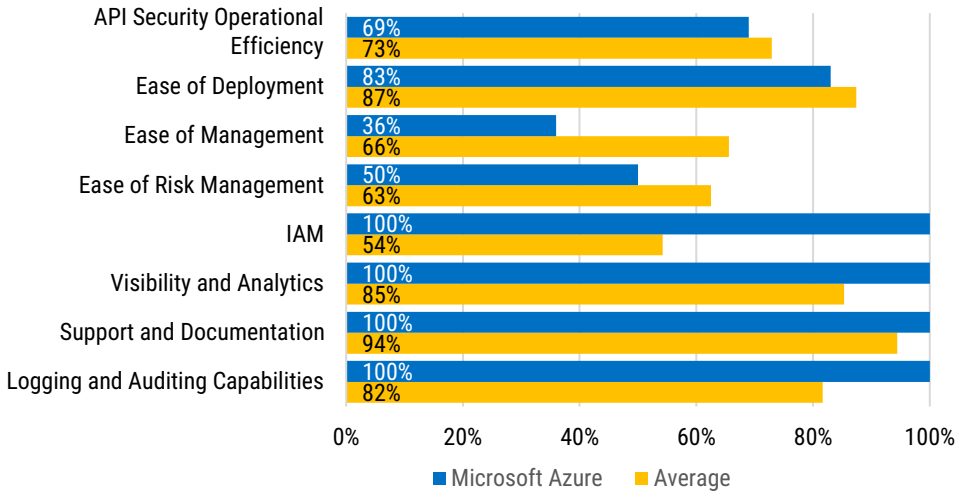


Figure 5. Overview of Operational Efficiency Results for Microsoft Azure API Security

Operational efficiency in deploying, managing, and utilizing WAAP solutions is critical for modern enterprises. WAAP solutions that provide WAF and API security with a high operational efficiency optimize resource allocation, minimize the burden on infrastructure, and reduce operational costs.

As to the first, SecureIQLab already validated WAF 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 4 above provides an overview of the operational efficiency results for the Microsoft Azure WAAP.

As to the second, in SecureIQLab's premiere validation of API security operational efficiency, seven categories are reviewed, within which a total of 37 features and functions are validated. These seven categories include Ease of Deployment, Ease of Management, Ease of Risk Management, Identity Access Management Control, Visibility & Analytics, Support and Documentation, and Logging & Auditing Capabilities. Figure 5 provides an overview of the operational efficiency findings for the API Security Platform.

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, med, or low. The *Operational Efficiency Rating* is equal to the total number of points scored respectively by the WAAP operational efficiency validation over the total number of points. Category scores were calculated by aggregating earned points and then dividing this number by the total number of possible points to find a percentage. Points (integers 0 – 3) are earned for each feature within a category as follows:

- High or Yes (Green) = 3 Points
- Med (Yellow) = 2 Points
- Low (Orange) = 1 Point
- NA/No (Red) = 0 Points

The *Operational Efficiency Rating* was calculated by adding together the total points for each category, then dividing this number by the maximum potential points (117) and multiplying that number by 100%. Equation 4 states the *Operational Efficiency Rating* calculation. The *API Security Operational Efficiency Rating* is calculated in a similar manner to the *Operational Efficiency* Rating using the percentage of the total points earned from the seven areas of validation to the 111 total points possible.

$$\text{Operational Efficiency Rating} = \frac{\left(\begin{array}{c}\text{Ease of Deployment}\\ \text{Points}\end{array} + \begin{array}{c}\text{Ease of Management}\\ \text{Points}\end{array} + \begin{array}{c}\text{Ease of Risk Management}\\ \text{Points}\end{array} + \begin{array}{c}\text{Scalable and Elastic}\\ \text{Points}\end{array} + \begin{array}{c}\text{Logging and Auditing}\\ \text{Points}\end{array}\right)}{117 \text{ points}} \times 100\%$$

Equation 4. Operational Efficiency Rating Calculation

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.

4.1. Web Application Firewall Operational Efficiency Details

The detailed results for SecureIQLab's validation of Microsoft's operational efficiency are found below in Table 8. Microsoft received an Operational Efficiency Rating of 91%, which is higher than the group average.

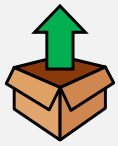
	WAF Operational Efficiency Test Case	Azure Rating	Group Average
	Simplicity of Provisioning	Medium	High
	Ease of Setting Up WAF Service	High	High
	Ease of Certificate creations and management	High	High
	Application Load Balancing and Monitoring	High	High
	Deployment Autonomy/customer support experience	High	High
	Integration with Multi-Cloud WAF	Yes	Yes
	Plug and Play Integration with On-prem Firewall	Yes	No
	Plug and Play Integration for SIEM/S3 Bucket	Yes	Yes
	Plug and Play Integration for API Gateway	Yes	Yes
	Ease of Deployment Rating	**96%**	**87%**
	Simplicity of Tuning WAF	High	High
	False Positive Resistant Pre-Canned Security Profile	High	High
	Intuitiveness of Security Policy	High	High
	Ease of Managing Security Policy	High	High
	Customization of Dashboard	High	High
	Capability of Asset Management	Low	Medium
	Facilitation of PCI Compliance	High	Medium
	Facilitation of Data Sovereignty (GDPR)	High	High
	WAF Update Automation	Medium	Medium
	Simplicity of Managing Web ACL	High	High
	Single Sign On Support	Yes	Yes
	Efficient User Management	High	Medium
	Ease of Management Rating	**92%**	**86%**
	Risk Assessment & Mitigation	Low	Medium
	Security Metrics Reporting	High	High
	Threat Analytics Dashboard	High	High
	Alert and Rule Management	High	High
	Automated Alert and Rule Management	Medium	Medium
	Incident Management	Low	Medium
	Ease of Risk Management Rating	**72%**	**84%**
	Load Balancing and Failover Capability	High	High
	Auto-Scaling Capability	Yes	Yes
	Manual Scaling Capability	Yes	No
	Designed for Static and Dynamic Sites	Yes	Yes
	Multi-tenancy Support	Yes	Yes
	Scaling and Elastic Capabiites Rating	**100%**	**82%**
	Log Configuration Simplicity	High	High
	Log Storage Capability	High	High
	Web Request Inspection	Medium	High
	Application Monitoring	High	Medium
	Infrastructure Monitoring	High	High
	Auditing Capability	Medium	Medium
	Multi-Factor Authentication	Yes	Yes
	Logging & Auditing Capabilites Rating	**90%**	**87%**
	WAF Operational Efficiency Rating	**91%**	**86%**

Table 8. Operational Efficiency Detailed Results

4.2. Application Programming Interface Security Operational Efficiency Details

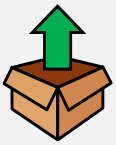
	API Security Operational Efficiency Validation Case	Azure Rating	Group Average
	API Technology Supported	High	High
	Speed for API Deployment	Medium	Medium
	Speed to Push the Policy	Medium	High
	Support for Multiple Deployments	High	High
	Ease of Deployment Rating	**83%**	**88%**
	API Endpoint Addition Support	NA	Medium
	API Endpoint Visibility	NA	Medium
	API Endpoint Discovery	NA	Low
	Default Template for Policy Management Support	High	Medium
	Speed to Discover All API Endpoints	NA	Low
	Violation ratings support	Medium	High
	Managing policies for API groups	Low	High
	Capability of dashboard to filter and export data	Low	Medium
	Intuitiveness of security policy	High	High
	Ease of tuning API security policies	High	High
	API Endpoint Classification Capability	NA	Low
	Visibility into different API versions	No	No
	Ease of Management Rating	**36%**	**66%**
	Alert on Implementation Malpractice	NA	Low
	Coverage for Top 10 OWASP List	Medium	Medium
	Rate Limiting Strategies to Manage Risks	High	High
	Speed to Patch API Security Signature	Medium	Low
	False Positive Mitigation Strategy Support	No	Yes
	Access Token Theft/Leakage Strategies	Medium	Low
	Ease of Risk Management Rating	**50%**	**63%**
	MFA Integration Support	Yes	No
	Role-Based Access Control Support	Yes	No
	SSO Integration Support	Yes	Yes
	Authentication and Authorization Mechanisms Support.	High	Medium
	Identity Management and Access Control	**100%**	**54%**
	Security Metrics Reporting	High	High
	Dashboard Customization	High	Medium
	Exporting of Security Metrics	High	High
	Visibility and Analytics	**100%**	**85%**
	Documentation for Installation in Public Domain	High	High
	Documentation for Best Practices Deployment	High	High
	Support for Knowledge Base	High	High
	Vendor Moderated Support Forum	High	High
	Private Channel for Communication with Support	High	High
	Support and Documentation	**100%**	**94%**
	API Application Monitoring Capabilities	High	Medium
	Logs Retention	High	Medium
	Log Export Capabilities	High	High
	Logging & Auditing Capabilities Rating	**100%**	**81%**
	API Operational Efficiency Rating	**69%**	**73%**

Table 9. API Operational Efficiency Results

As Table 9 demonstrates, while Microsoft's API operational efficiency is slightly lower than average, they scored perfect scores in four of the seven categories.[10]

5. False Positive Avoidance

WAAPs need to allow business-related transactions while blocking malicious activity. Blocking legitimate user activity constitutes a false positive, increases the operational burden for the enterprise and requires additional tuning to correct.

Properly tuned security devices will not detect benign traffic as malicious. More than 6,500 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 being protected by the cloud WAAP. The results for the *False Positive Avoidance* testing are found below in Table 10. The higher the *False Positive Avoidance Score*, the less impact on the operational efficiency.

Microsoft's *False Positive Avoidance Score* is the percentage of the total allowed legitimate activity test cases to the total test cases.

False Positives	Azure Results	Group Average
False Positive Avoidance Score	100.0%	99.98%

Table 10. False Positive Avoidance Score

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%. Microsoft achieved a perfect score and performed above the group average.

6. Differentiators

Microsoft provided the following information to highlight their market differentiators:

> Microsoft is one of the biggest privately owned WAN and fiber secure network infrastructures, offering more than 200 services.
>
> Microsoft has experience in managing and securing traffic at scale from large Microsoft global online services like LinkedIn, Bing, O365 for many years.
>
> Microsoft has strong investments in security with a large internal threat intelligence community and is supported by thousands of security professionals.
>
> Microsoft provides native integrations with other Microsoft Security services, including Azure Firewall Manager, Microsoft Sentinel, etc.
>
> Microsoft has Automated Deployment: Azure WAF can be deployed and configured as part of your IaC practices, allowing for automated, consistent, and repeatable deployments across environments.
>
> Azure WAF is designed to scale with your applications, providing high availability and resilience without compromising on security.

[10] The Microsoft Azure API Management (APIM) solution, not tested in this iteration, may provide additional advanced API security capabilities and features when integrated with the Microsoft Azure WAF and API Security solution.

7. Conclusion

The Microsoft Azure Web Application Firewall and API Security performed well in both security efficacy and operational efficiency. Microsoft's *Complete Security Score* of 87.65% and Operational *Efficiency Rating* of 91% are both better than the averages. Microsoft blocked all Layer 7 DoS and DDoS attacks. Microsoft performed significantly better than average in resiliency testing. Additionally, Microsoft earned four perfect scores in API operational efficiency categories. These remarkable scores were earned while generating zero false positives throughout the test cycle.

As one of the seven vendors that successfully passed the WAAP vulnerability assessment with a score of 100%, The Microsoft Azure Web Application Firewall and API Security earned SecureIQLab's rating of "Secure by Design".

8. Appendix

Please see the linked appendix here.

9. Contact Information

SecureIQLab, LLC.
9600 Great Hills Trail Suite #150W
Austin, TX 78759 USA
+1.512.575.3457

www.secureiqlab.com
info@secureiqlab.com

10. Copyright and Disclaimer

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

SecureIQLab (May 2024)