SecureIQlab®

Public Test Report

Cloud WAAP CyberRisk Validation Report – Fortinet

Product Version:	**FortiWeb Web Firewall VM AMI-AWS 7.40build**
Language:	**English**
Published:	**9 May, 2024**

Contents

1. Executive Summary 2
2. Introduction 3
3. Security Efficacy 3
   3.1. OWASP Top 10 Validation 4
      3.1.1. OWASP Web Application Firewall Score 4
      3.1.2. OWASP Application Programming Interface Security Rating 5
   3.2. Advanced Threat Coverage 6
      3.2.1. Bot Attacks 7
      3.2.2. Layer 7 DoS Attacks 7
      3.2.3. Resiliency Score 8
      3.2.4. WAAP Vulnerability Assessment 8
4. Operational Efficiency 9
   4.1. Web Application Firewall Operational Efficiency Details 10
   4.2. Application Programming Interface Security Operational Efficiency Details 12
5. False Positive Avoidance 13
6. Differentiators 13
7. Conclusion 15
8. Appendix 15
9. Contact Information 15
10. Copyright and Disclaimer 16

1. Executive Summary

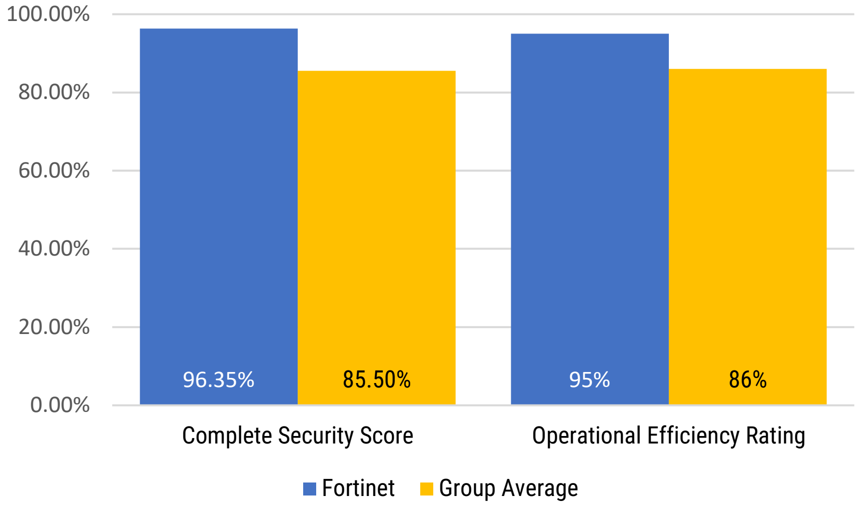


Figure 1. Overall Validation Results for Fortinet a Cloud WAF and API Security

This report discusses the test results for the Software as a Service (SaaS) Fortinet Cloud WAF 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 Fortinet Cloud WAAP was markedly superior to 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, ease of 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 Fortinet Cloud WAF and API Security overall validation results. Fortinet earned the third top *Complete Security Score* with a score of 96.35% and the second top *Operational Efficiency Score* with a score of 95%, which are significantly higher 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

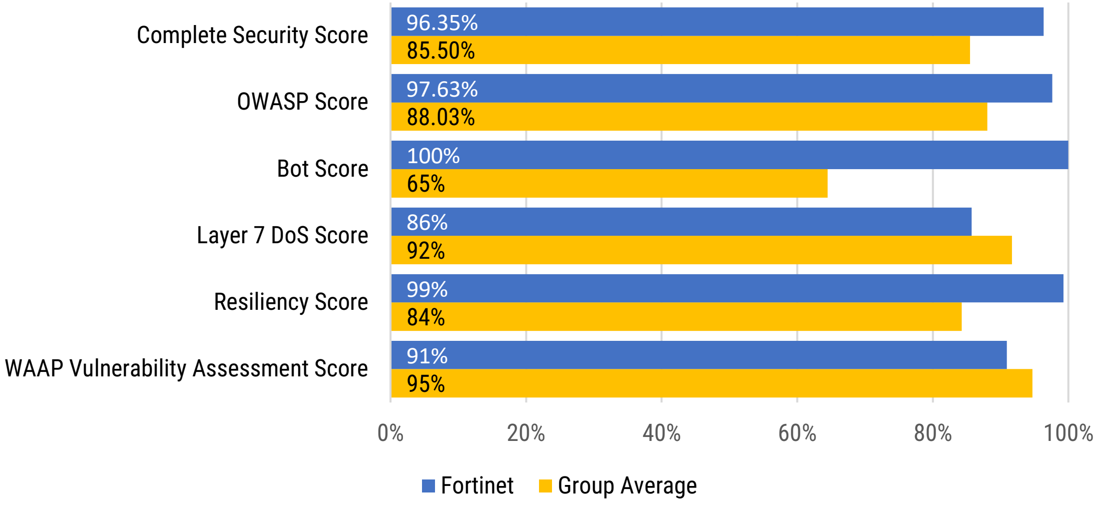


Figure 2. Security Validation Results for Fortinet WAAP

Figure 2 above provides an overview of the SecureIQLab findings during the security validation of the Fortinet Cloud WAAP. To summarize, SecureIQLab's testing demonstrates the efficacy of the Fortinet Cloud 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	Fortinet %Blocked/Score	Group Test Average
A01:2021-Broken Access Control	Path Traversal	99.0%	99.5%
	CSRF	100.0%	52.8%
A02:2021-Cryptographic Failures	Cryptographic Failures	100.0%	100.0%
A03:2021-Injection	XPath Injection	86.7%	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)	71.2%	73.3%
	Cross Site Scripting (XSS)	100.0%	99.7%
	LDAPi	100.0%	79.5%
	SSTI	66.7%	83.1%
	PHP Code Injection	100.0%	96.9%
A04:2021-Insecure Design	Web Scraping(Parse Hub)	0.0%	50.0%
	LFI	100.0%	71.1%
	RFI	100.0%	87.8%
A05:2021-Security Misconfiguration	Unrestricted File Upload (UFU)	100.0%	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	95.2%	87.1%
A10:2021-Server-Side Request Forgery (SSRF)	SSRF	100.0%	76.4%
OWASP WAF Score		**97.63%**	**88.03%**

Table 1. OWASP WAF Vulnerability Testing

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

[6] SecureIQLab is not affiliated with OWASP.

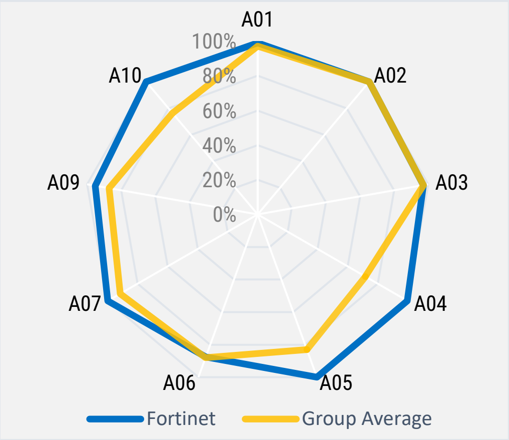


Figure 3. Comparative OWASP WAF Coverage for Fortinet vs Group Average

The Fortinet Cloud 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 Fortinet 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.

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

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.

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

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, Fortinet demonstrated superior security coverage over the 9 OWASP categories tested. Fortinet scored 100% in 14 out of the 21 validated test cases and scored considerably better than 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 for 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	Fortinet Rating (1-5)	Group Average (1-5)
API1:2023 - Broken Object Level Authorization	5	2.7
API2:2023 - Broken Authentication	5	2.3
API3:2023 - Broken Object Property Level Authorization	3	2.8
API4:2023 - Unrestricted Resource Consumption	2	2.7
API5:2023 - Broken Function Level Authorization	5	2.3
API6:2023 - Unrestricted Access to Sensitive Business Flows	5	3.7
API7:2023 - Server Side Request Forgery	3	2.3
API8:2023 - Security Misconfiguration	2	2.0
API9:2023 - Improper Inventory Management	3	2.8
API10:2023 - Unsafe Consumption of APIs	5	5.0
OWASP API Rating	**3.8**	**2.9**

Table 2. OWASP API Security Rating Results

Protocols Tested	Fortinet Rating (1-5)	Group Average (1-5)
REST-API	5	3.2
GraphQL	2	3.2
SOAP	5	3.4
Kubernetes	5	3.5
WebSockets	5	1.9
gRPC[8]	1	2.3
API Security Rating	**3.8**	**2.9**

Table 3. API Security Results for Tested Protocols

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 Fortinet's above average scores in both OWASP API Security protection and various protocols test categories. 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 includes Bot Attacks, Layer 7 DoS

[8] Fortinet notes that the gRPC test cases were executed using HTTP/1.1, a less common deployment but still in use. Fortinet highlights its ability to fulfill these use cases when assessed over HTTP/2, a common practice for gRPC today.

Attacks, Resiliency, and WAAP Vulnerability Assessment.

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. Fortinet's Cloud 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	Fortinet Results	Group Average
Web Crawler	Blocked	67%
Broken Link Checker	Blocked	67%
User Agent Manipulation	Blocked	50%
Bot Score	**100%**	**65%**

Table 4. Bot Attack Results

Table 4 shows Fortinet received a perfect score in Bot Protection and performed considerably 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 Fortinet's Cloud 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	Fortinet Results	Group Average
DDoS - LOIC	Blocked	83%
Slowhttptest Slow Header (-H)	Blocked	92%
Slowhttptest Slow Body (-B)		83%
Slowhttptest Slow Read (-X)	Blocked	100%
Torshammer	Blocked	92%
MHDDoS	Blocked	92%
Slowloris	Blocked	100%
Layer 7 Dos Score	**86%**	**92%**

Table 5. Layer 7 DoS Results

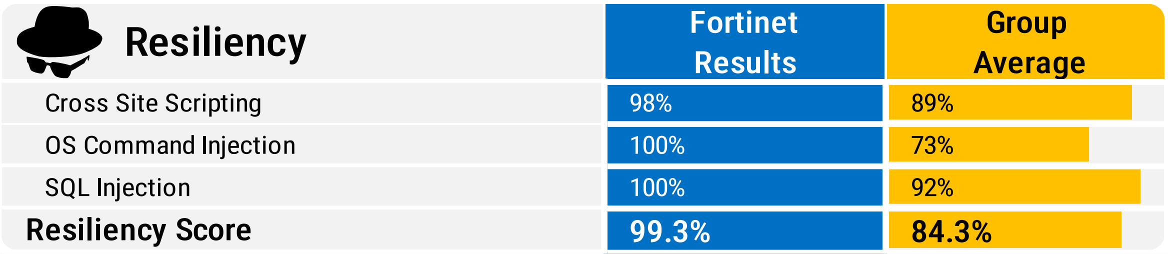
Fortinet blocked both of the Layer 7 DDoS attacks and four out of five of the Layer 7 DoS attacks, earning an 86% score.

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 Fortinet Cloud 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 Fortinet Cloud 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%.

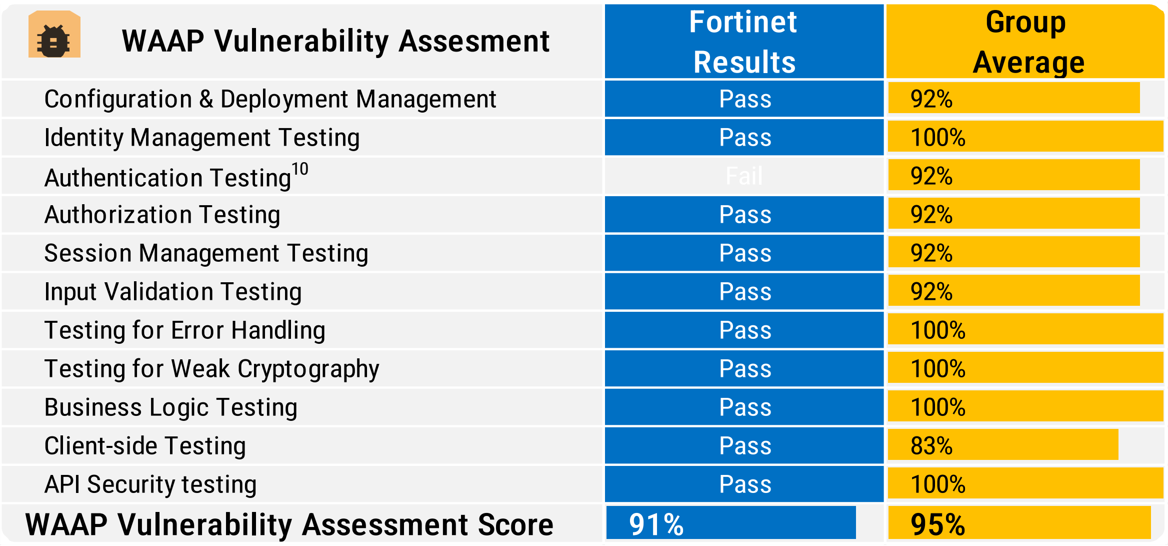


Resiliency	Fortinet Results	Group Average
Cross Site Scripting	98%	89%
OS Command Injection	100%	73%
SQL Injection	100%	92%
Resiliency Score	**99.3%**	**84.3%**

Table 6. Resiliency Validation Results

Fortinet achieved the maximum *Resiliency Score* among all vendors tested.

3.2.4. WAAP Vulnerability Assessment



WAAP Vulnerability Assesment	Fortinet Results	Group Average
Configuration & Deployment Management	Pass	92%
Identity Management Testing	Pass	100%
Authentication Testing[10]	Fail	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	**91%**	**95%**

Table 7. WAAP Vulnerability Assessment Results

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

[10] Fortinet's password policy provides flexible configuration options for password complexity, enabling customers to tailor 'password policy' requirements specific to their security needs. This ensures that users comply with their unique password requirements.

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.

Fortinet 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%.

Fortinet achieved 91% score in the WAAP vulnerability assessment.

4. Operational Efficiency

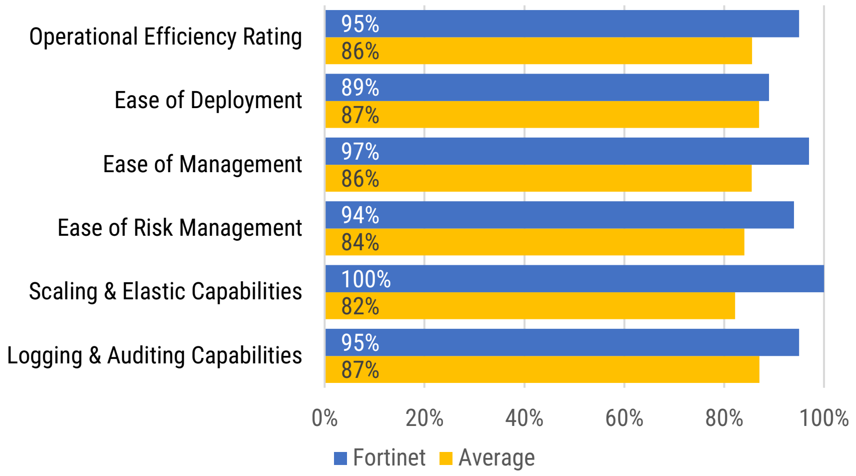


Figure 4. Overview of Operational Efficiency Results for Fortinet Cloud Web Application Firewall

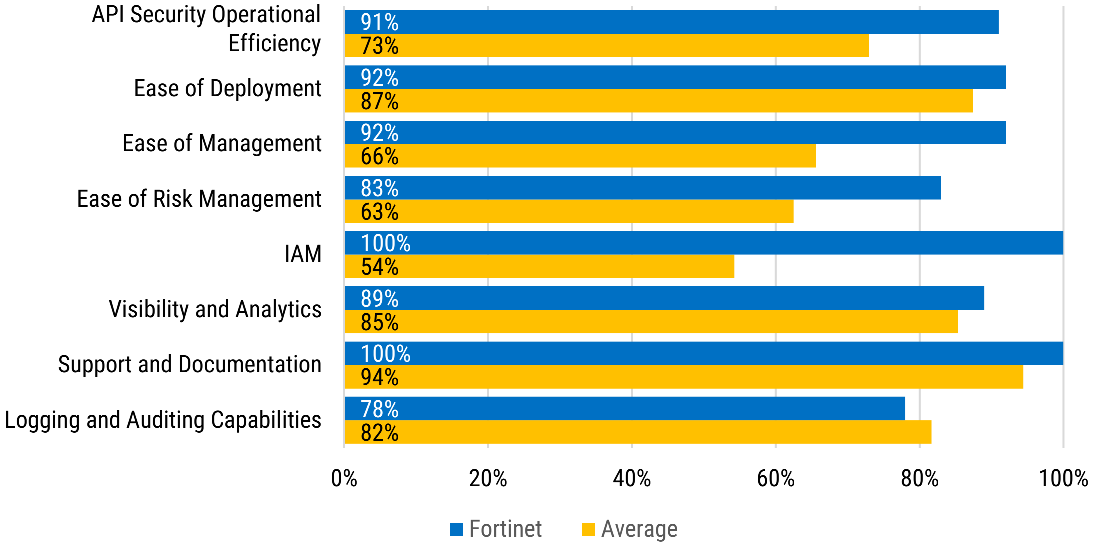


Figure 5. Overview of Operational Efficiency Results for Fortinet Cloud API Security

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 has already validated the operational efficiency of WAF in five areas of validation, covering a total of 39 features and functions. 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 Fortinet Cloud WAAP. Fortinet achieved the second top score of 95% among all vendors tested.

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.

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

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 Fortinet's operational efficiency are found below in Table 8. Fortinet received the second highest score for operational efficiency and was notably higher than the group average.

WAF Operational Efficiency Test Case	Fortinet Rating	Group Average
Simplicity of Provisioning	Medium	High
Ease of Setting Up WAF Service	Medium	High
Ease of Certificate creations and management	High	High
Application Load Balancing and Monitoring	High	High
Deployment Autonomy/customer support experience	Medium	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	89%	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	Medium	High
Capability of Asset Management	High	Medium
Facilitation of PCI Compliance	High	Medium
Facilitation of Data Sovereignty (GDPR)	High	High
WAF Update Automation	High	Medium
Simplicity of Managing Web ACL	High	High
Single Sign On Support	Yes	Yes
Efficient User Management	High	Medium
Ease of Management Rating	97%	86%
Risk Assessment & Mitigation	High	Medium
Security Metrics Reporting	High	High
Threat Analytics Dashboard	Medium	High
Alert and Rule Management	High	High
Automated Alert and Rule Management	High	Medium
Incident Management	High	Medium
Ease of Risk Management Rating	94%	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	Medium	High
Log Storage Capability	High	High
Web Request Inspection	High	High
Application Monitoring	High	Medium
Infrastructure Monitoring	High	High
Auditing Capability	High	Medium
Multi-Factor Authentication	Yes	Yes
Logging & Auditing Capabilites Rating	95%	87%
WAF Operational Efficiency Rating	95%	86%

Table 8. Operational Efficiency Detailed Results

4.2. Application Programming Interface Security Operational Efficiency Details

API Security Operational Efficiency Validation Case	Fortinet Rating	Group Average
API Technology Supported	High	High
Speed for API Deployment	Medium	Medium
Speed to Push the Policy	High	High
Support for Multiple Deployments	High	High
Ease of Deployment Rating	**92%**	**88%**
API Endpoint Addition Support	High	Medium
API Endpoint Visibility	High	Medium
API Endpoint Discovery	NA	Low
Default Template for Policy Management Support	High	Medium
Speed to Discover All API Endpoints	High	Low
Violation ratings support	High	High
Managing policies for API groups	High	High
Capability of dashboard to filter and export data	High	Medium
Intuitiveness of security policy	High	High
Ease of tuning API security policies	High	High
API Endpoint Classification Capability	High	Low
Visibility into different API versions	Yes	No
Ease of Management Rating	**92%**	**66%**
Alert on Implementation Malpractice	Medium	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	Yes	Yes
Access Token Theft/Leakage Strategies	High	Low
Ease of Risk Management Rating	**83%**	**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	Medium	Medium
Exporting of Security Metrics	High	High
Visibility and Analytics	**89%**	**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	Low	Medium
Logs Retention	High	Medium
Log Export Capabilities	High	High
Logging & Auditing Capabilities Rating	**78%**	**81%**
API Operational Efficiency Rating	**91%**	**73%**

Table 9. API Operational Efficiency Results

As Table 9 demonstrates, Fortinet's API operational efficiency achieved the top score among all vendors tested.

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 in Table 10. The higher the *False Positive Avoidance Score*, the less impact on the operational efficiency.

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

False Positives	Fortinet 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%. Fortinet achieved a perfect score in False Positive Avoidance.

6. Differentiators

Fortinet provided the following information to highlight their market differentiators:

> FortiWeb is a web application firewall (WAF) that protects web applications and APIs from attacks that target known and unknown exploits and helps maintain compliance with regulations. Using machine learning to model each application, FortiWeb defends applications from known vulnerabilities and from zero-day threats. High performance physical, virtual appliances, and containers deploy on-site or in the public cloud to serve any size of the organization—from small businesses to service providers, carriers, and large enterprises.
>
> **<u>FortiWeb Differentiators</u>**
>
> **Web Application Protection:** FortiWeb provides complete security for your web-based applications from the OWASP Top 10 and many other threats. FortiWeb's first layer of defense uses traditional WAF detection engines (e.g. attack signatures, IP address reputation, protocol validation, and more) to identify and block malicious traffic, powered by intelligence from Fortinet's industry leading security research from FortiGuard Labs. FortiWeb's machine learning detection engine then examines traffic that passes this first layer, using a continuously updated model of your application to identify malicious anomalies and block them as well.
>
> **API Protection:** FortiWeb web application firewall provides the right tools to address threats to APIs. FortiWeb API Discovery and Protection uses machine learning algorithms to automatically discover APIs by continuously evaluating application traffic. Discovery is an integral role for

establishing a positive security model and FortiWeb protects your critical APIs based on your profiled API inventory. FortiWeb can also integrate out of the box policies together with an automatically generated positive security model policy that is based on your organization's schema specification (OpenAPI, XML and generic JSON are supported schemas) to protect against API exploits. FortiWeb schema validation can be integrated into the CI/CD pipeline, automatically generating an updated positive security model policy once the API is updated.

Bot Mitigation: FortiWeb protects against automated bots, webs scrapers, crawlers, data harvesting, credential stuffing and other automated attacks to protect your web assets, mobile APIs, applications, users and sensitive data. Combining machine learning with policies such as threshold based detection, Bot deception and Biometrics based detection with superior good bot identification FortiWeb is able to block malicious bot attacks while reducing friction on legitimate users. With advanced tracking techniques FortiWeb can differentiate between humans, automated requests and repeat offenders, track behavior over time to better identify humans from bots and enforce CAPTCHA challenges when required. Together with FortiView, FortiWeb's graphical analysis dashboard organizations can quickly identify attacks and differentiate from good bots and legitimate users.

Security Fabric Integration: As the threat landscape evolves, many new threats require a multi-pronged approach for protecting web-based applications. Advanced Persistent Threats that target users can take many different forms than traditional single-vector attack types and can evade protections offered only by a single device. FortiWeb's integration with FortiGate and FortiSandbox extend basic WAF protections through synchronization and sharing of threat information to both deeply scan suspicious files and share infected internal sources. FortiWeb also provides integration with leading third-party vulnerability scanners to provide dynamic virtual patches to security issues in application environments. Vulnerabilities found by the scanner are quickly and automatically turned into security rules by FortiWeb to protect the application until developers can address them in the application code.

FortiWeb's Machine Learning: FortiWeb's multi-layer approach provides two key benefits: superior threat detection and improved operational efficiency. FortiWeb's ability to detect anomalous behavior relative to the specific application being protected enables the solution to block unknown, never-before-seen exploits, providing your best protection against zero-day attacks targeting your application. Operationally, FortiWeb machine learning relieves you of time-consuming tasks such as remediating false positives or manually tuning WAF rules. FortiWeb continually updates the model as your application evolves, so there is no need to manually update rules every time you update your application. FortiWeb enables you to get your code into production faster, eliminating the need for time-consuming manual WAF rules tuning and troubleshooting the false positives that plague less advanced WAFs.

FortiGuard Services: Fortinet's Award-winning FortiGuard Labs is the backbone for many of FortiWeb's layers in its approach to application security. Offered as five separate options, you can choose the FortiGuard services you need to protect your web applications. FortiWeb IP address reputation service protects you from known attack sources like botnets, spammers, anonymous proxies, and sources known to be infected with malicious software. FortiWeb Security Service is designed just for FortiWeb including items such as application layer signatures, machine learning threat models, malicious robots, suspicious URL patterns, and web vulnerability scanner updates. Credential Stuffing Defense checks login attempts against FortiGuard's list of compromised credentials and can take actions ranging from alerts to blocking logins from suspected stolen user ids and passwords. The FortiWeb Cloud Sandbox subscription enables FortiWeb to integrate with Fortinet's cloud-sandbox service. Finally, FortiWeb offers FortiGuard's top-rated antivirus engine that scans all file uploads for threats that can infect your servers or other network elements.

7. Conclusion

The Fortinet Cloud WAF and API Security performed remarkably well in both security efficacy and operational efficiency. Fortinet's *Complete Security Score* of 96.35% is the third-highest score earned and is significantly better than the average score. Fortinet's *Operational Efficiency Rating* of 95% is the second top score and is notably better than average. Additionally, Fortinet's *WAF OWASP score* is in the top three, with a score of 97.63%, and achieved the top Resiliency score among all vendors tested. These remarkable scores were earned while generating a perfect score in false positives throughout the test cycle.

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

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

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

SecureIQLab (May 2024)