SecureIQlab®

2022 Cloud Web Application Firewall (WAF) CyberRisk Return on Security Investment (ROSI) Report - StackPath

Published: January 19, 2023

Version: Essentials Package

Report Contents:

1 Introduction

The remote workforce has dissolved the network perimeter. This, along with cost savings and operational simplicity, is driving organizations to adopt cloud infrastructure. The explosive adoption of the cloud comes with associated risks. For example, web application-based vulnerabilities are among the top breach vectors[1]. Cloud-based web application firewalls (WAFs) are designed to mitigate this risk by protecting applications without interrupting business operations in a cloud-first world. Cloud-based web application firewalls (WAFs) should accurately detect, prevent, and log attacks while remaining resistant to false positives. In addition, WAFs should provide auditing capabilities, meet regulatory compliance requirements, and enable business continuity.

SecureIQLab conducted an exhaustive test of 14 enterprise class web application firewall (WAF) products[2] to determine their security efficacy, operational efficiency, and return on security investment (ROSI). The full comparative report is available here. Individual reports for each of the 14 WAF solutions tested are also available here.

In the course of this test, the products were subjected to a battery of diverse attacks. Simple ecommerce applications and multiuser web applications were used as targets. Test cases were based upon industry frameworks and regulatory requirements, such as the OWASP Top 10[3] and PCI DSS[4]. The resultant data was obtained while securing targeted cloud applications hosted on AWS, Azure, GCP, and Oracle.

The vendors and tested products were selected based on meeting one or more of the following three criteria:

1. Market Leaders: Either in terms of revenue generated, customer numbers globally, or strong channel play
2. Analyst and Enterprise challengers: Small-mid-large enterprise security professional surveys, Direct 1:1 Inquiries and engagement with enterprises, organizations, MSP's, MSSP's and Gartner MQ, buyers guide, Forrester Wave, and IDC reports
3. New market entrants and interested participating vendors: Challengers claiming breakthrough technology offerings

This report highlights the Return on Security Investment (ROSI) and additional Total Cost of Ownership (TCO) related metrics that result from using the StackPath WAF Essentials Package with the purchase of an additional 39M requests per month. The purchase of the additional requests per month is required to meet SecureIQLab WAF testing specifications. The StackPath WAF Essentials package and The StackPath's WAF Professional package, used in the original evaluation, have the same test results. (The Professional package natively complies with our testing standards.) This report is the result of post-publication communications with StackPath and was created to highlight ROSI related metrics derived from another valid WAF package and its pricing.

[1] https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/summary-of-findings/

[2] Testing was attempted on a total of 17 cloud WAF solutions. See Appendix section 8.8 for details.

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

[4] https://blog.pcisecuritystandards.org/pci-dss-v4-0-resource-hub

2 Return On Security Investment

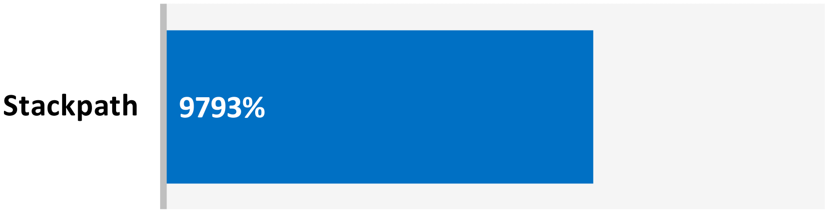

Figure 1. Return on Security Investment

Return On Security Investment (ROSI) differs from the traditional Return On Investment (ROI) in that ROSI is calculated on the bases of prevented losses and not generated income. The Security Effectiveness (SE), Operational Efficiency (OE), *Annual Product Cost* (APC), and Annual Loss Expectancy (ALE) are all used in the calculation of the ROSI in Figure 1. Equation 1 demonstrates how ROSI is calculated by SecureIQLab.

- *Security Effectiveness* (SE): Security solutions with higher security efficacies will stop more threats and help to prevent more losses. *Complete Security Scores* in decimal format are used as SE values in our ROSI calculations.
- *Annual Total Cost of Ownership* (TCO)*:* The total cost of the security solution is the APC plus the *Annual Operational Expense* for the solution. See Appendix, section 5.6 for TCO calculation.
- *Annual Loss Expectancy* (ALE): Anticipated annual financial loss related to security incidents. This is unique to each organization and may be extrapolated from historical losses. SecureIQLab uses an ALE equal to $4.24M[5] in calculating ROSI[6].

$$ROSI = \frac{ALE \times SE - TCO}{TCO}$$

Equation 1. ROSI Calculation

3 CyberRisk Ripple[7]

The CyberRisk Ripple combines SE, TCO, and ALE. The computation required to generate the CyberRisk Ripple is broken down in the following sections.

3.1 Annual Total Cost of Ownership

First, let's look at *Annual Total Cost of Ownership*, sorting products into high (large markers), medium (medium sized markers) and low categories (small markers). An *Annual Total Cost of Ownership* less than $35,000[8] is in the low category, an TCO less than $46,000[9] is in the medium category and all TCOs above $46,000 are in the high category.

[5] https://www.ibm.com/reports/data-breach
[6] Based on one breach per year
[7] All colors in figures and tables in this section do not indicate quality.
[8] Determined by Average TCO – STDEV/2, rounded to the nearest $1000.
[9] Determined by Average TCO + STDEV/2, rounded to the nearest $1000.

This leads to the following Table 1:

Vendor	TCO	Complete Security Score vs. ROSI Graph Marker	Operational Efficiency Rating vs. ROSI Graph Marker
Stackpath	Low	●	▲

Table 1. Annual Total Cost of Ownership[10]

Because StackPath was evaluated in both categories, it has both a circle and a triangle. In this calculation, both markers for StackPath are small. The round marker is used for the subsequent Figure 2 and Figure 4 graphs. The triangular marker is used for the subsequent Figure 3 and Figure 4 graphs.

TCO is essential because it helps organizations budget appropriately for the optimal products for their security and operational requirements.

3.2 Complete Security Score vs. ROSI

The relation between *Complete Security Score* and Return on Security Investment (ROSI) is shown in the following graph.

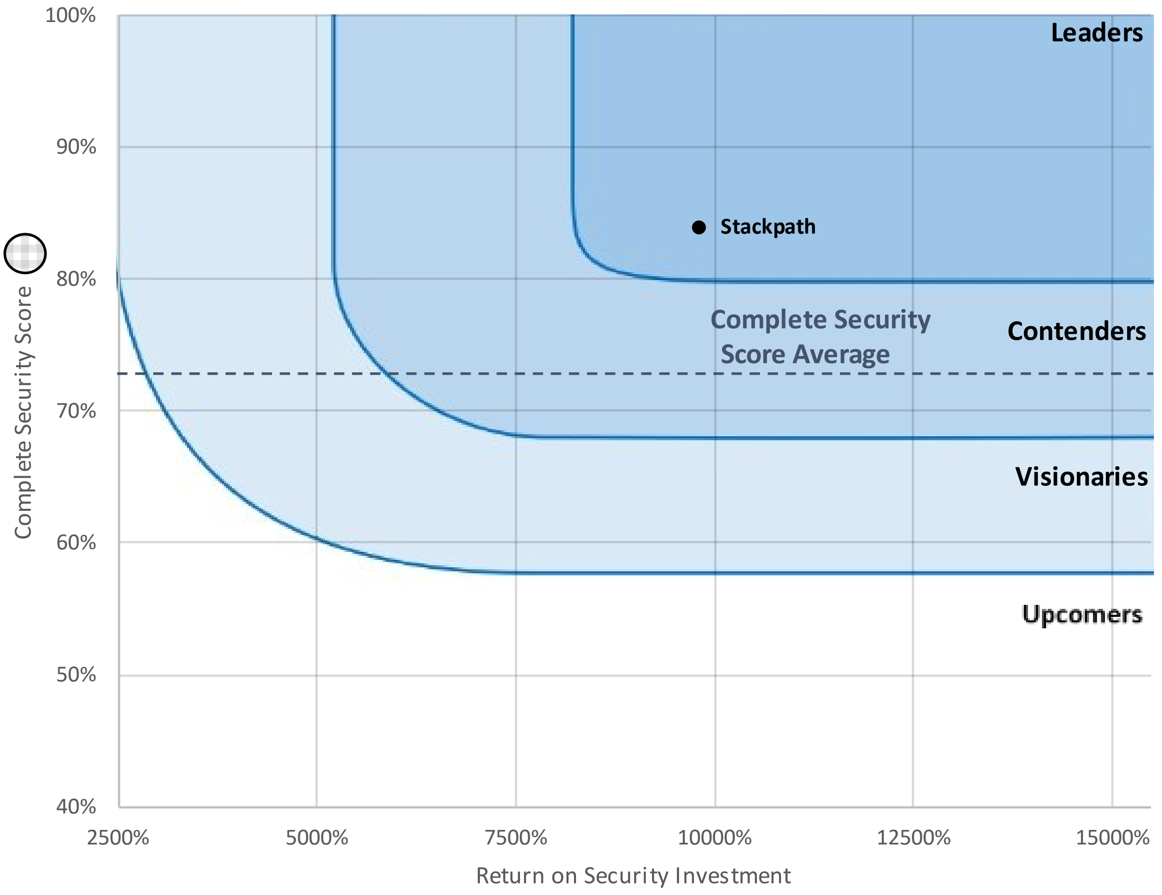

Figure 2. CyberRisk Security Efficacy Ripple

[10] See Appendix 5.6 for additional details on Total Cost of Ownership

As seen in the above graph, four categories for Security Efficacy in figure 2 are derived from the results of the *Operational Efficiency Scores, Security Efficacy Scores* and ROSI[11]. These four categories are:

- ***Leaders***: These Cloud WAF solutions demonstrated a combination of superior security and ROSI. That is, these solutions provide stronger security technology at competitive pricing. *Security Efficacy Leaders* have an above average ROSI and a *Complete Security Score* greater than the average of the *Operational Efficiency* and *Security Efficacy Scores.*
    - StackPath Essentials is a *Security Efficacy Leader.*
- ***Contenders*****:** These Cloud WAF solutions demonstrated excellent prevention and detection capabilities, delivering with an attractive ROSI, befitting small-to-medium enterprises and businesses. *Security Efficacy Contenders* have a ROSI value greater than the average ROSI – one standard deviation and a *Complete Security Score* greater than one standard deviation below the average of the *Operational Efficiency* and *Security Efficacy Scores.*
- ***Visionaries*****:** These Cloud WAF solutions demonstrated either excellent security or ROSI. That is, solutions in this category were priced competitively or provided better than average security. *Security Efficacy Visionaries* have a ROSI value greater than the average ROSI – two standard deviations and a *Complete Security Score* greater than two standard deviations below the average of the *Operational Efficiency* and *Security Efficacy Scores.*
- ***Upcomers***: These Cloud WAF solutions demonstrated lower Security Efficacy standards which contributed to lower ROSI. *Security Efficacy Upcomers* have a ROSI value less than the average ROSI – two standard deviations or a *Complete Security Score* less than two standard deviations below the average of the *Operational Efficiency* and *Security Efficacy Scores.*[12]

[11] A Security Efficacy Leader ranking for a product is no guarantee that the product will meet your specific security requirements.

[12] Products ranked as *Security Efficacy Upcomers* may still meet business-specific security use case requirements.

3.3 Operational Efficiency Score vs. ROSI

Third, we compare between *Operational Efficiency* and ROSI. The Y-axis labels are found on the right of the graph because we are going to combine this graph with the prior graph when we synthesize the results.

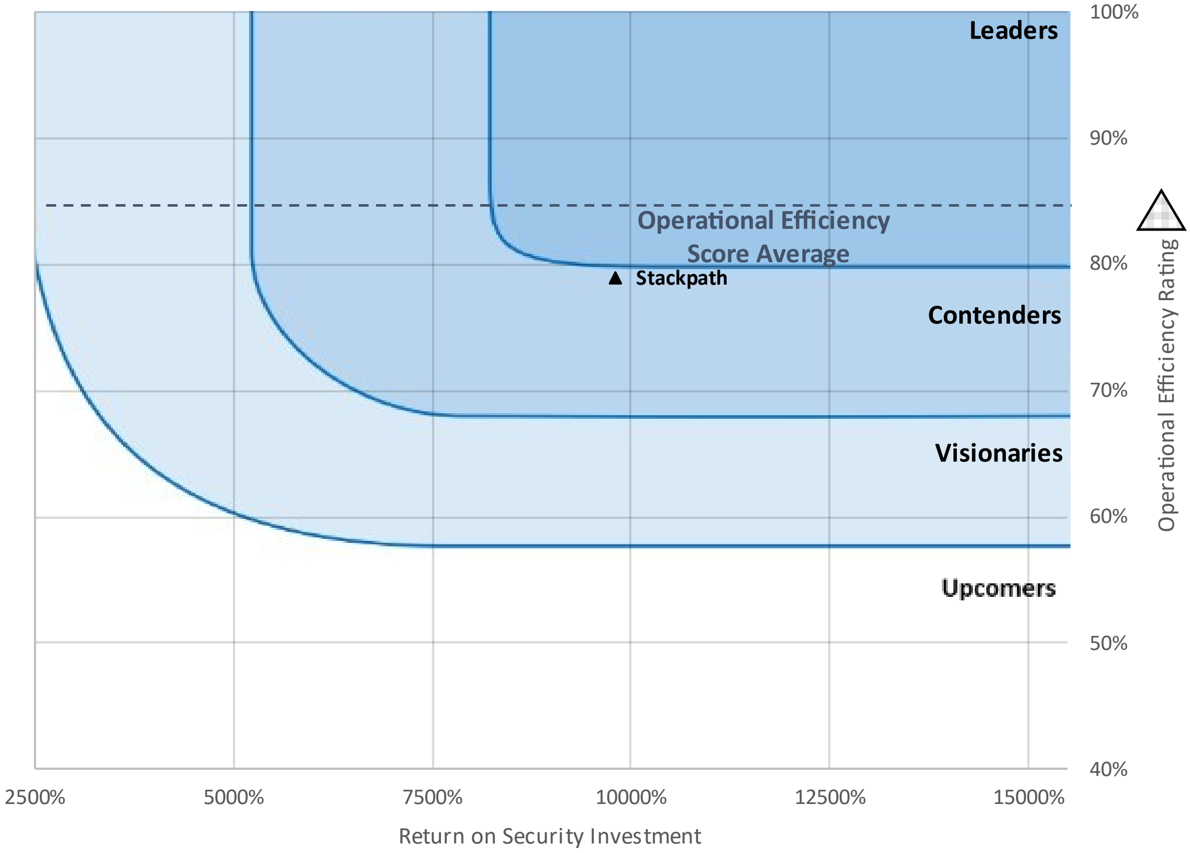

Figure 3. CyberRisk Operational Efficiency Ripple

Figure 3 allows us to determine that cloud web application firewalls as a group have a more mature operational efficiency than overall security efficacy. In addition, four categories for *Operational Efficiency* are derived from the results of the *Operational Efficiency Scores, Security Efficacy Scores* and ROSI[13]. These four categories are:

- ***Leaders***: These cloud WAF solutions demonstrated a combination of high-grade operational efficiency and superior ROSI. That is, these solutions combine ease of deployment, integration and resource management at competitive pricing. *Operational Efficiency Leaders* have an above average ROSI and an *Operational Efficiency Score* greater than the average of the *Operational Efficiency* and *Security Efficacy Scores.*
- ***Contenders***: These Cloud WAF solutions demonstrated excellent operational efficiency when it came to ease of deployment, integration and strike a good balance between the technology and resource management with an attractive ROSI. *Operational Efficiency Contenders* have a ROSI value greater than the average ROSI – one standard deviation and an *Operational Efficiency Score* greater than one standard deviation below the average of the *Operational Efficiency* and *Security Efficacy Scores.*
  - StackPath Essentials is an *Operational Efficiency Contender.*
- ***Visionaries***: These Cloud WAF solutions demonstrated good operational efficiency standards when it came to ease of deployment, integration or an excellent ROSI. *Operational Efficiency Visionaries* have a

[13] An Operational Efficiency Leader ranking is no guarantee that the product will meet your specific operational requirements.

ROSI value greater than the average ROSI – two standard deviations and an *Operational Efficiency Score* greater than two standard deviations below the average of the *Operational Efficiency* and *Security Efficacy Scores.*

- ***Upcomers***: These Cloud WAF solutions demonstrated lower operational efficiency standards when it came to ease of deployment, integration and struck a lower balance between the technology and resource management, delivering a lower ROSI. *Operational Efficiency Upcomers* have a ROSI value less than the average ROSI – two standard deviations or an *Operational Efficiency Score* less than two standard deviations below the average of the *Operational Efficiency* and *Security Efficacy Scores.*[14]

3.4 2022 Cloud WAF CyberRisk Ripple

Assembling the previous data into one figure yields:

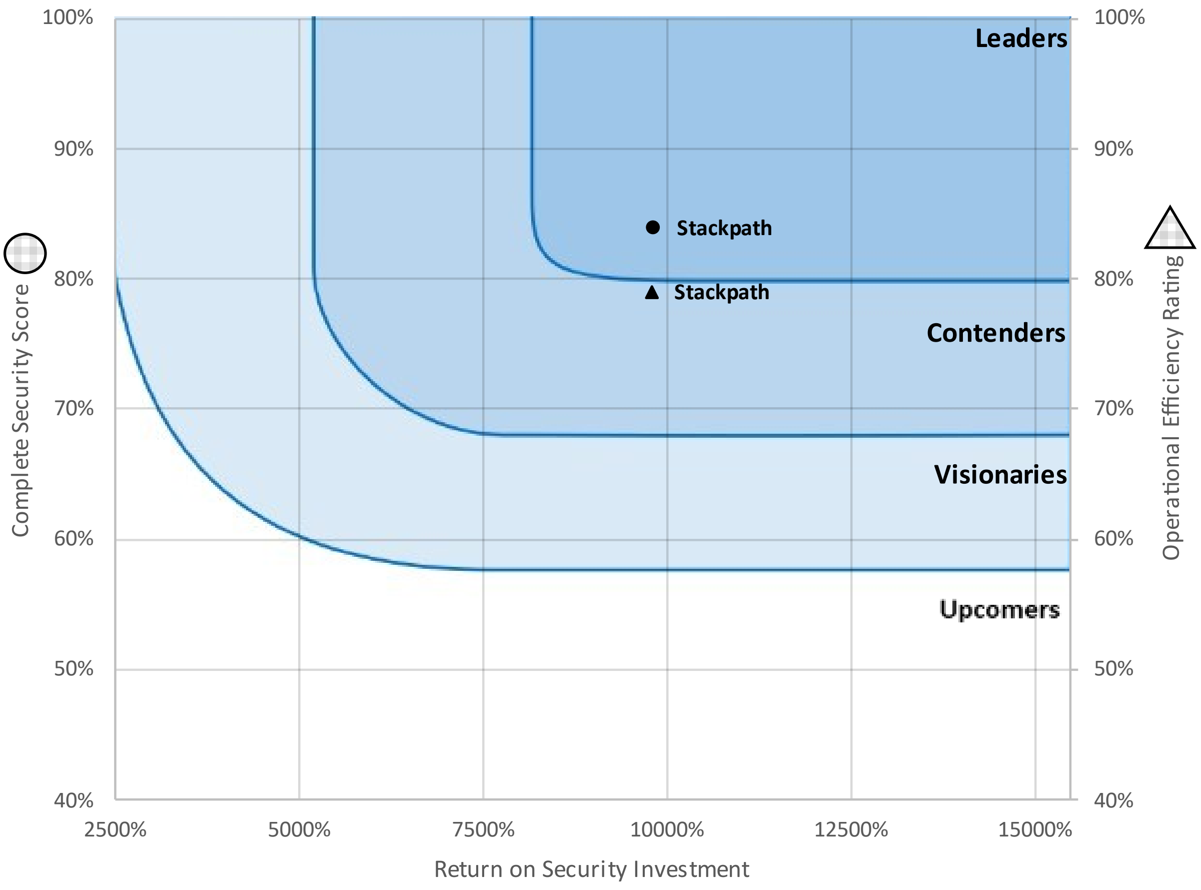

Figure 4. SecureIQLab Cloud WAF CyberRisk Ripple

The SecureIQLab Cloud WAF CyberRisk Ripple, Figure 4, is the culmination of an exhaustive and detailed approach to cloud WAF testing and validation research. This figure plots the Complete Security Score with circular markers and the Operational Efficiency Score with triangular markers versus ROSI. The upper right corner highlights the best operational efficiency, security efficacies and ROSI. Small markers indicate lower *Total Cost of Ownership*, medium sized markers indicate medium *Total Cost of Ownership*, and larger markers indicate a higher *Total Cost of Ownership*.

[14] Products ranked as *Operational Efficiency Upcomers* may still meet business-specific operational use case requirements.

By way of comparison, Figure 5 below is the figure from our 2022 Cloud Web Application Firewall (WAF) CyberRisk Validation Comparative Report updated with the StackPath WAF Essentials package scores.

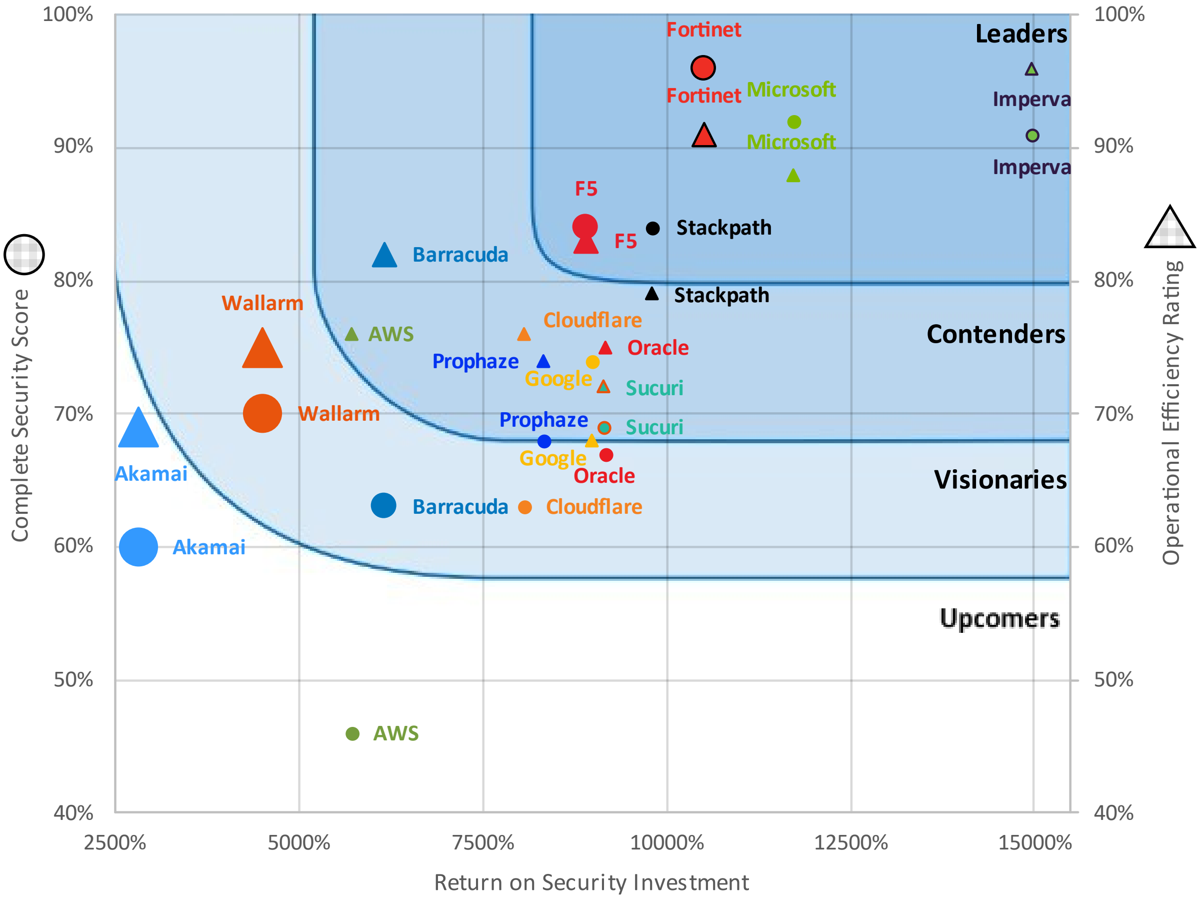

Figure 5. StackPath WAF Essentials Package CyberRisk Ripple Comparative Results[15]

4 Conclusion

Summarizing the data from the previous section we get Table 2.

Vendor	Security Efficacy	Operational Efficiency
StackPath	Leader	Contender

Table 2. SecureIQLab's Cloud WAF CyberRisk Ripple Results

Testing evolves with the changing IT and threat landscapes. Each test iteration provides additional insight into how the WAF industry and individual vendors evolve to address operational business requirements. The 2021 Cloud WAF CyberRisk testing provided a baseline for cloud WAF industry performance. The 2022 Cloud WAF CyberRisk test provides readers with a second evaluation of security efficacy, operational efficiency, and the resultant ROSI for popular cloud WAF solutions.

[15] Figure 8 of the 2022 Cloud Web Application Firewall (WAF) CyberRisk Validation Comparative Report.

SecureIQLab's individual test reports and comparative test report offer details for each of the vendors tested. Still, every organization's attack surface, business requirements, and risk mitigation strategy are unique, so thorough evaluation of cloud WAF technologies before deployment is essential.

5 Appendix

5.1 Cloud WAF Test Deployment

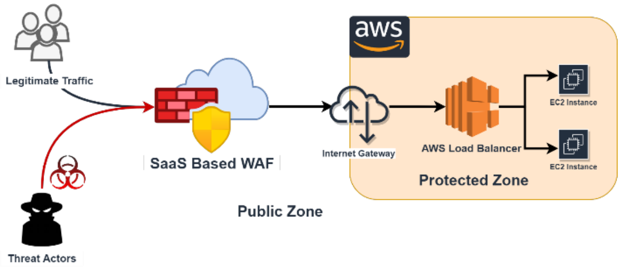

Figure 6. SaaS WAF Deployment

The StackPath WAF was deployed with default policies[16] with elastic load balancers to protect the web-applications on AWS, Figure 6. All web-application transactions were inspected by the cloud WAFs. In doing so, the cloud WAFs were expected to provide protection against threats by malicious actors while allowing intended usage of application resources.

During deployment, our engineers noted the time it took to deploy with out of the box controls and the complexity of the deployment. Also noted was whether our engineering team was required to contact the WAF vendor's support team to successfully complete the WAF deployment.

5.2 Test Execution

SecureIQLab performed security validation using crafted attacks that are relevant to today's cloud application hosted on cloud and cloud native applications. SecureIQLab carefully curated such attacks via research generated by our own red team as well as the attacks that are prevalent in the wild. Open-source tool kits were also utilized while performing this assessment.

Before the testing was conducted, SecureIQLab validated that the cloud WAF solution was in an operational state by verifying the following:

Connection Validation:

1. Before any test is conducted, SecureIQLab ensures that the Cloud WAF can be accessed by the administrator and is passing normal application traffic. This is to ensure that any dynamic content such as IP blacklist protection can be updated on regular basis by the cloud WAF.

Logging:

2. SecureIQLab understands that logging is a critical and crucial component while running a cloud WAF. SecureIQLab verifies that the cloud WAF being tested will have sufficient administrative as well as attack logging to ensure Security Analyst can troubleshoot and fix issues as required.

[16] Please see Appendix 5.4 Product Configuration and Appendix 5.5 Product Rules for deployment details.

Updates:

3. Protocol updates in the form of rules, signatures and reputations will be applied as they become generally available. SecureIQLab will make best effort to apply these updates to the products prior to the evaluation.

The above processes were repeated wherever applicable throughout the test. Once the deployment of the WAF solution and baseline testing were completed, the security validation testing began.

The first phase of attack was to gather information and perform reconnaissance against the application. The was done to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. SecureIQLab performed vulnerability analysis using automated tools such as Burpsuite and Nessus in addition to performing manual analysis. The main objective of vulnerability analysis is to discover flaws in the systems and applications which can be leveraged by an attacker. These flaws ranged anywhere from host and service misconfiguration to insecure application design. Vulnerability Analysis was based on:

1. Active Scan: Active scan involves direct interaction with the component being tested for security vulnerabilities.
2. Passive Scan: Passive scan involves meta-data analysis and traffic monitoring.

Once information gathering and reconnaissance was completed, we began exploitation as the next phase in this process. Penetration testing was critical in the evaluation of cloud WAF technologies.

Once exploited, "post-exploitation" was undertaken. Post-exploitation refers to the actions taken after the initial compromise of a system or device. It often describes the methodical approach of using privilege escalation or pivoting techniques—which allowed SecureIQLab, in this case, to establish a new source of attack from the new vantage point in the system—to gain additional access to systems or network resources. We demonstrate the risk presented by exploitable systems and what post-exploitation may likely occur with web applications.

Additionally, defense evasion is an important tool in an attacker's arsenal. This allows old methods and techniques to be repurposed to evade protection against attacks which might otherwise get blocked by the Cloud WAF.

The testing demonstrates the effectiveness of the product under test (PUT) to protect vulnerable assets from targeted threats and exploitation. This asset/target and threat-based approach forms the basis from which the PUT security effectiveness is measured.

5.3 Attack Types

The SecureIQLab threat and attack suite contains attacks (including mutations of the same underlying attacks) and proprietary exploits harvested through our test harness or crafted by our threat research team. SecureIQLab has a number of complex web applications which have also been constructed to include known vulnerabilities and coding errors. Based on the intended attack, groups of exploits are carefully selected from this library to test. Each exploit has been validated to impact the target vulnerable host(s) by compromising the asset, which can range from the web server, the web application, to the site. The level of compromise can include instigating a denial-of-service (DoS) condition, providing administrator/root access to the host server, allowing malicious users to amend system parameters or application data before submission, browsing and/or retrieving files stored on the host server, or escalating user privileges.

5.4 Product Configuration

Cloud WAF products were deployed and configured according to the default instructions found on the vendors' websites and, where applicable, on cloud infrastructure providers' marketplaces.

5.5 Product Rules

Cloud WAF products were configured according to the default instructions found on the vendors' websites and, where applicable, on cloud infrastructure providers' marketplaces. Default rule sets were used for 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.

Any further required tuning to deploy in the test environment was performed according to publicly available vendor recommendations to replicate the customer experience during the deployment and management of the product. (Enterprises are advised to exercise due diligence during this process to avoid impacting business.)

5.6 Product Pricing[17]

Normalized pricing for products tested is listed in Table 6. Product pricing models varied in complexity, from one monthly fee to an à la carte feature set, prorated hourly, model.[18] There were also significant variations in pricing structure and feature set combinations[19] between all 14 vendors tested.[20] In order to best compare the variety of options tested, the pricing options used are normalized[21] to support a minimum of:

- 1 TB of data per month
- 40 million requests monthly
- 1 site being protected

Normalized pricing was also calculated based on the product being enabled for the entire month, fees being paid monthly where required[22], and protection against botnet attacks[23] being included. Lastly, cloud infrastructure costs for the virtual deployment models are included in the normalized pricing.

Vendor	Normalized Price	Annual TCO
Stackpath	$5,400	$34,433

Table 6. Normalized Pricing and Annual Total Cost of Ownership

The Annual Total Cost of Ownership (TCO) is the *Annual Product Cost* (APC) of the WAF solution plus the weighted *Annual Operational Expense* (AOE) for the product. The APC is the *Normalized Price*. The *Annual Operational Expense* is the cost of one full-time employee that spends 10% of their time supporting the WAF product, divided by the decimal format for the *Operational Efficiency Rating* (OE) and the *False Positive Avoidance Score* (FPA). Equation 2 depicts the TCO calculation.

$$TCO = APC + \frac{AOE}{OE \times FPA}$$

Equation 2. Calculation of TCO

The cost of the full-time employee is based on a $75/hr rate and includes overhead. For the purpose of this report, the total cost of the employee comes to $225k/year.

5.7 Methodology

The test was conducted in accordance with the standards of the Anti-Malware Testing Standards Organization (AMTSO). The test used version 2.0 of the SecureIQLab Cloud WAF CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP054).

Tests were performed utilizing black-box and gray-box testing. Black-box testing assumes that the internal code

[17] Support tiers and offerings vary by vendor and may need to be considered for budgetary purposes. Prices for support are not included in pricing.
[18] Pricing will vary.
[19] Vendor standard feature sets may change with time.
[20] Pricing is dynamic.
[21] Pricing normalization may cause pricing variance with vendor list pricing.
[22] Some vendors offer incentives for annual and multi-year commitments.
[23] Botnet protection is not a standard feature for all products.

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 a WAF can be complex. Tuning was based on industry and marketplace expectations that these solutions will require minimal to no tuning during provisioning, deployment, and management phases, which 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).

Further, any required tuning was performed according to publicly available vendor recommendations, to replicate the customer experience during the deployment and management of the product. (Enterprises are advised to exercise due diligence during this process to avoid impacting business.) Browsing the WAF-protected applications was performed using standard user transactions that included form submissions, comment writing, ecommerce transactions, and other transactions.

The Anti-Malware Testing Standards Organization (AMTSO) is an international nonprofit association that focuses on addressing the global need for improvement in the objectivity, quality, and relevance of anti-malware testing methodologies. SecureIQLab is a member of AMTSO.

The Open Web Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. "Through community-led open-source software projects, hundreds of local chapters worldwide, tens of thousands of members, and leading educational and training conferences, the OWASP Foundation is the source for developers and technologists to secure the web."[24] It publishes the OWASP Top 10 Report. SecureIQLab has no affiliation with OWASP.

More detailed information about our testing methods is contained in version 2.0 of the SecureIQLab Cloud WAF CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP054).

6 Contact Information

SecureIQLab is a cybersecurity testing lab that was founded in 2019. SecureIQLab works with enterprises, governments, and security vendors to bridge the applied intelligence gap that exists between market and technology research. SecureIQLab also provides services to operationalize security and the metrics to help organizations improve their return on security investments.

SecureIQLab, LLC.
6001 W. Parmer Lane Ste 370, #970
Austin, TX 78704 USA

+1.512.575.3457

www.secureiqlab.com
info@secureiqlab.com

[24] https://owasp.org/

7 Copyright and Disclaimer

SecureIQLab cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the research results cannot be taken by any representative of SecureIQLab. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering research results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, research documents or any related data.

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

SecureIQLab (January 2023)