SecureIQlab™

Bridging the enterprise cloud security gap

Cloud Web Application Firewall (WAF) CyberRisk Validation Comparative Report

Published: December 14, 2021

Language: English

www.secureiqlab.com

Report Contents:

1. INTRODUCTION 2
2. TESTING PARAMETERS AND RESULTS 3
    1. Security Results Overview 4
    2. Security Results Details 5
3. OPERATIONAL EFFICIENCY 6
    1. Operational Efficiency Results Overview 6
    2. Operational Efficiency Details 7
4. RETURN ON SECURITY INVESTMENT 8
5. CYBERRISK QUADRANT 9
    1. Price 9
    2. Complete Security Score vs. ROSI 10
    3. Operational Efficiency Score vs. ROSI 11
    4. Synthesis 13
6. CONCLUSION 13
7. APPENDIX 14
    1. Cloud WAF Test Deployment 14
    2. Test Execution 14
    3. Attack Types 15
    4. Product Configuration 16
    5. Product Rules 16
    5. Product Pricing 16
8. CONTACT INFORMATION 17
9. COPYRIGHT AND DISCLAIMER 17

SecureIQLab
Bridging the enterprise cloud security gap

1. INTRODUCTION

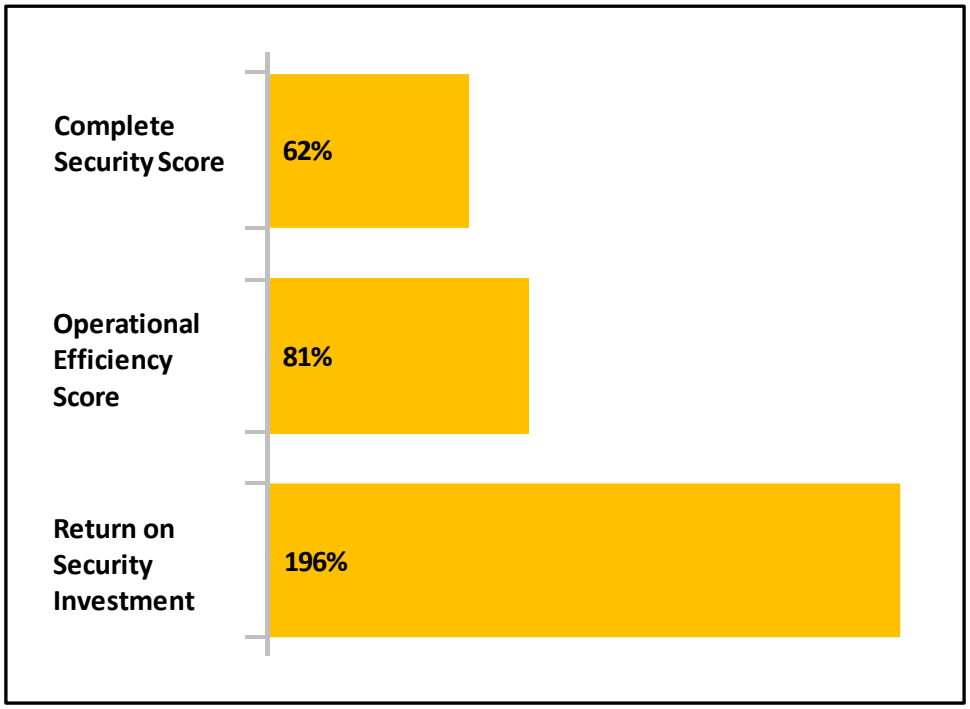

Figure 1. Overall Averages for the Nine Validated Products

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 web applications without interrupting business operations in the cloud first world.

SecureIQLab has conducted a groundbreaking test of nine web application firewall (WAF) products to determine their security and operational efficiency. This comparative report summarizes test results and provides a comparative overview of the nine products tested. This provides an at-a-glance comparative between the individual products under test and the collective results. Individual reports that highlight the performance of each of the nine vendors WAF solutions are also available.

This comparative report is a summary because thousands of attacks were simulated during the test against each of the nine products tested. Accordingly, Test results have necessarily been simplified and presented for review by small and medium-sized businesses, enterprises, and managed service providers (MSPs). Figure 1 provides a summary of the products' overall collective average validation results in broad categories.

During the test, products were subjected to a battery of diverse attacks. Simple ecommerce applications and multiuser web applications were used as targets. Empirically validated data based upon industry guidelines and regulations such as the OWASP Top 10[2] and PCI DSS[3] was obtained. It was obtained while securing targeted cloud applications on AWS with cloud WAFs.

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

[2] Open Web Application Security Project®

[3] Payment Card Industry Security Standards Council

The test was conducted in accordance with the standards of the Anti-Malware Testing Standards Organization[4] (AMTSO). The test used version 1.0 of the SecureIQLab Cloud WAF CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP039).

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

The Anti-Malware Testing Standards Organization (AMTSO) is an international non-profit 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."[5] It publishes the OWASP Top 10 Report. SecureIQLab has no affiliation with OWASP.

The nine vendors and tested products were selected for validation based on vendor feedback and their meeting one 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
1. New market entrants and interested participating vendors: Challengers claiming breakthrough technology offerings

2. TESTING PARAMETERS AND RESULTS

Cloud-based web application firewalls (WAFs) should accurately detect, prevent, and log attack attempts while remaining resistant to false positives. The aim of this section is to demonstrate the efficacy of the nine tested cloud WAF products in this area.

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.

Any required tuning was performed according to standard vendor recommendations available on the Vendor website and according to relevant documentation available on AWS Marketplace to align with what an organization would experience during use of the product.

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, that is, SMBs, managed service providers (MSPs), and managed security service providers (MSSPs). Tuning a WAF can be complex. Enterprises are advised to exercise due diligence

[4] https://www.amtso.org/
[5] https://owasp.org/

during this process to avoid impacting normal browsing of the web applications or normal web application transactions.

Browsing the WAF-protected applications was performed using standard user transactions that included form submissions, comment writing, ecommerce transactions, and other transactions. See Appendix Section 5 for additional information on the ruleset utilized during this test.

More detailed information about our testing methods is contained in version 1.0 of the SecureIQLab Cloud WAF CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP039).

1. Security Results Overview

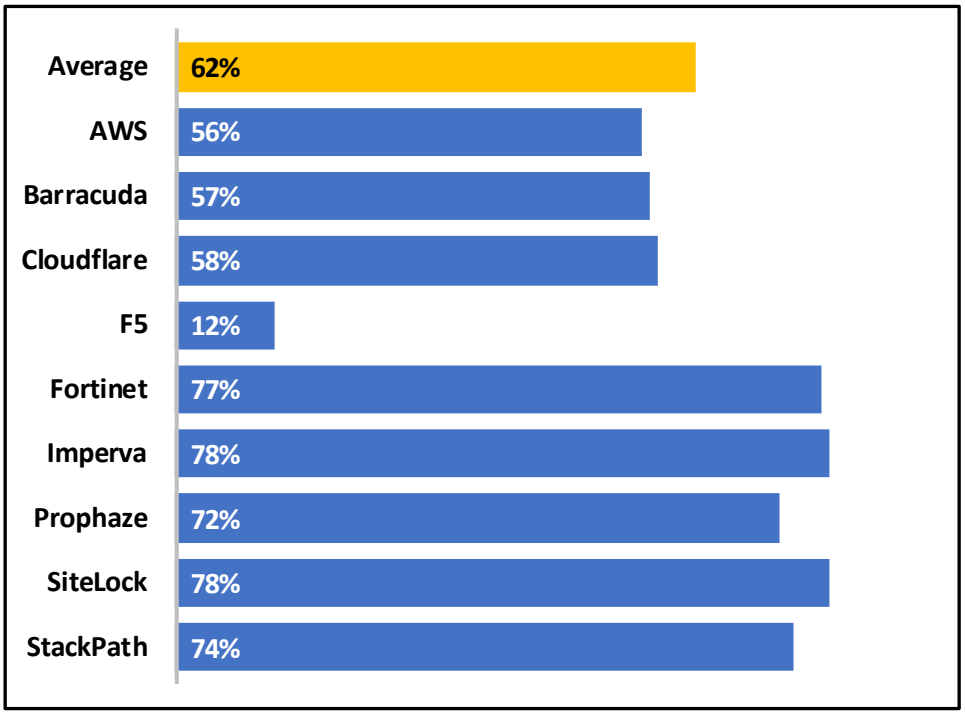

Figure 2. Comparative for Complete Security Scores

Figure 2 above provides an overview comparative of the SecureIQLab findings during security validation of the tested products. The *Complete Security Score* depicts the percentage of all attacks blocked by the WAF versus the total number of attacks tested. Equation 1 below depicts the *Complete Security Score* calculation, which is based on an unweighted percentage of all attacks blocked.

Complete Security Score = 100% x (All Attacks Blocked)/(Total Attacks)

Equation 1. Calculation of Complete Security Score

The calculation method in Equation 1 is unweighted to avoid the philosophical—and highly subjective—debate that invariably accompanies attack weighting. However, a necessary corollary to this is that threats that take more variations of simulated attacks to review will influence the Complete Security Score more than threats that can be evaluated with a lesser number of simulated attacks.

Every cloud WAF evaluated in this test was subjected to more than 100 real world-based operational scenarios targeting small-to-medium businesses and enterprises alike. A grand total of 22,465 attacks were used encompassing these scenarios and categories. The depth and scope of the testing performed by SecureIQLab is a first in the cybersecurity industry. SecureIQLab will continue to add attack libraries and other relevant operational metrics in future iterations of this test.

2. SECURITY RESULTS DETAILS[6]

Security efficacies were determined for five domains. Detailed explanations and results for each of these domains are provided in the individual test reports[7]. Table 1 provides an overview of testing results.

Vendor	Complete Security Score	OWASP	Resiliency	Botnet	Layer 7 dos	Vul. Web Environment
AWS	56%	64%	40%	71%	100%	100%
Barracuda	57%	73%	100%	100%	100%	100%
Cloudflare	58%	69%	100%	100%	100%	100%
F5	12%	47%	100%	86%	100%	*
Fortinet	77%	58%	*	71%	100%	*
Imperva	78%	85%	80%	100%	100%	100%
Prophaze	72%	60%	*	57%	100%	100%
SiteLock	78%	65%	80%	100%	100%	100%
StackPath	74%	79%	40%	86%	100%	100%
Average	62%	67%	60%	86%	100%	78%

Table 1. Security Efficacy Results

[6] Based on OWASP 2017 categories. Future test iterations are projected to use OWASP 2021 categories.

* Contact SecureIQLab for Details

[7] Individual test reports available at https://secureiqlab.com/publications/

3. Operational Efficiency[8]

1. Operational Efficiency Results Overview

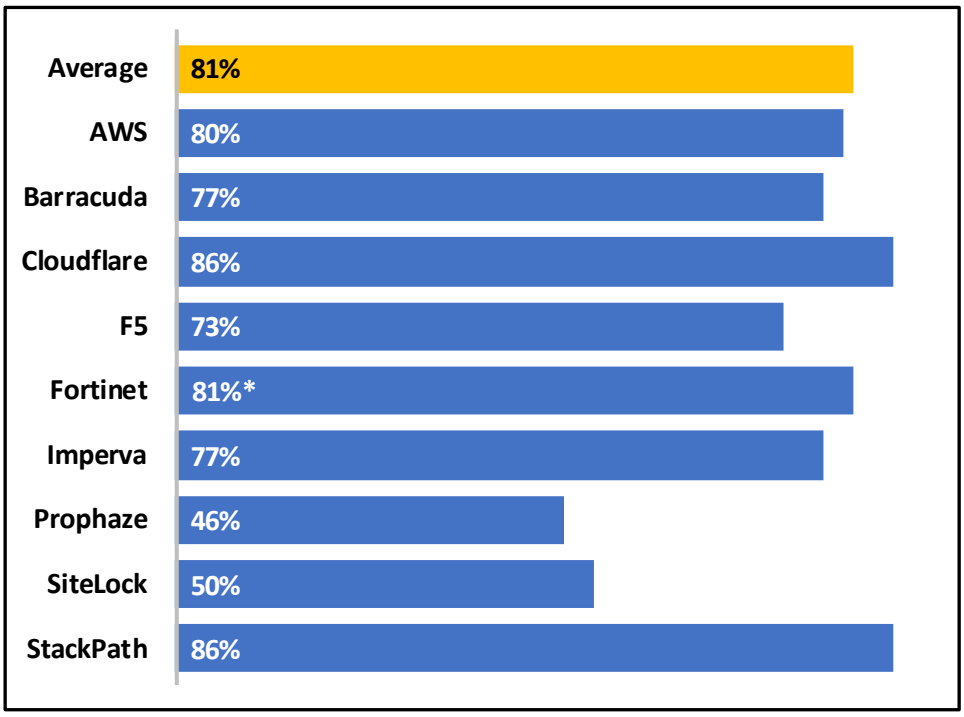

Figure 3. Comparative for Operational Efficiency Scores

Cloud-based WAF technology allows for the creation of customized security, which benefits organizations in the following ways:

- Ease of deployment and integration
- Less complex to manage
- Scalable and elastic
- Monitoring, logging, and control capabilities
- Allows business-related transactions

All nine products were validated in each of these areas of operational efficiency. Figure 3, above, provides a comparison of the resulting *Operational Efficiency Scores*.

Category scores were calculated by aggregating earned points and then dividing this number by the total possible score to find a percentage. Points (integers 0 – 3) are earned for each feature within a category. Results highlighted in green are worth three points; results highlighted in yellow are worth two points; results highlighted in orange are worth one point; and results highlighted in red are worth zero points.

As set forth in Equation 2 below, the *Operational Efficiency Score* was calculated by adding together the total points for each category, then dividing this number by the maximum potential points (84) and multiplying that number by 100%. Below, Equation 2 states the *Operational Efficiency Score* calculation.

[8] Fortinet operational efficiency reflected here is for FortiWEB-AWS.

$$\text{Operational Efficiency Score} = \frac{\left(\text{Deployment and Ease of Integration Points} + \text{Management Complexity Points} + \text{Scalable and Elastic Points} + \text{Logging and Auditing Points} + \text{False Positive Points}\right)}{\text{84 Points}} X\ 100\%$$

Equation 2. Operational Efficiency Score Calculation

Validation average results are determined by either calculating the mean results or taking the mode from the vendor group results where relevant. Mean results are taken when the results are quantitative, e.g., *Time to Deploy, # of Steps for Setting up WAF service or # Audit Trail Fields*. The mode is used in the group average results when the results are qualitative in nature, e.g., *Complexity of Tuning WAF, Auto-Scaling Capability or Log Configuration Complexity.*

2. Operational Efficiency Details

Operational efficiency was determined for five different areas of use. Detailed explanations and results for each of these five areas are provided in the individual test reports[9]. Table 2 provides an overview of our operational validation.

Vendor	Operational Efficiency Score	Deployment and Ease of Integration	Management Complexity	Scalable and Elastic	Logging and Auditing	False Positive
AWS	80%	70%	89%	89%	81%	100%
Barracuda	77%	67%	89%	100%	71%	100%
Cloudflare	86%	91%	67%	100%	86%	100%
F5	73%	76%	61%	78%	71%	100%
Fortinet	81%	76%	100%	56%	81%	100%
Imperva	77%	91%	67%	22%	86%	100%
Prophaze	46%	55%	67%	*	29%	100%
SiteLock	50%	55%	67%	*	43%	100%
StackPath	86%	79%	83%	100%	90%	100%
Average	81%	79%	67%	100%	86%	100%

Table 2 Operational Efficiency Results

[9] Individual test reports available at https://secureiqlab.com/publications/

4. Return On Security Investment

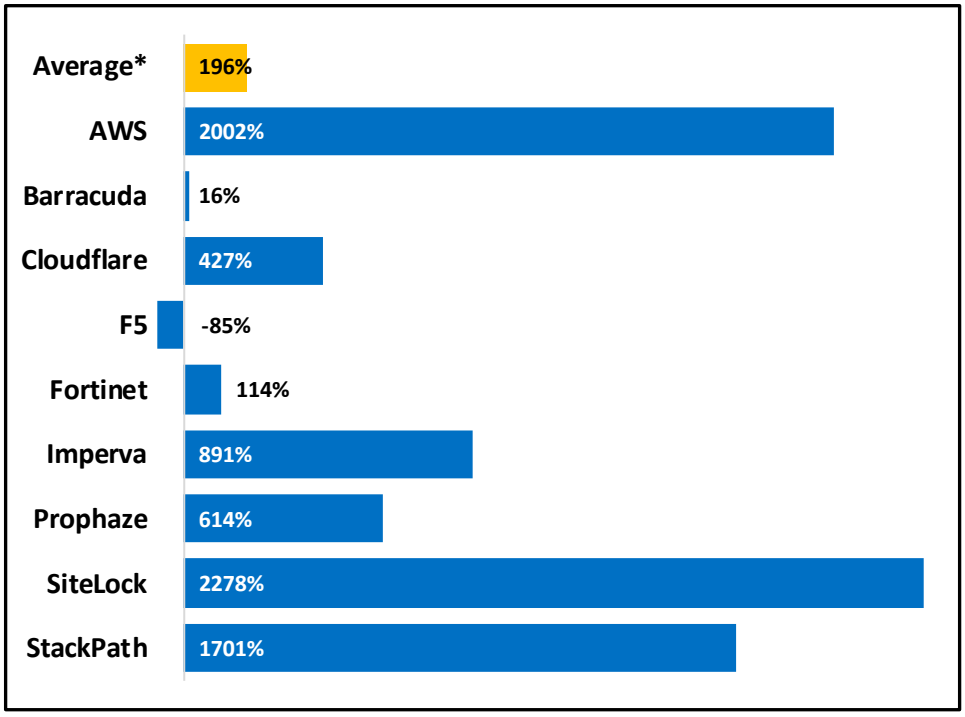

Figure 4. Return on Security Investment

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 ROSI in Figure 4. Equation 3 demonstrates how ROSI is calculated by SecureIQLab.

- *Security Effectiveness* (SE): Security solutions with higher security efficacies will stop more threats and prevent more loss. *Complete Security Scores* divided by 100% are used as SE values in our ROSI calculations.
- *Operational Efficiency* (OE): Products with a higher *Operational Efficiency Score* will require less overhead to use and will facilitate incident resolution. *Operational Efficiency Scores divided by 100%* are used for OE values.
- *Annual Product Cost* (APC): Total cost of the security solution annually. See Appendix, Table 3 for pricing details.
- *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 $25,612 in calculating ROSI.[10]

$$ROSI = \frac{ALE \times SE \times OE - APC}{APC}$$

Equation 3. ROSI Calculation

* Average ROSI calculated from average price, average *Security Efficacy Score*, and the average *Operational Efficacy Score*.

[10] Hiscox, an international specialist insurer, reports that average annual losses related to security incidents for small businesses to be approximately $25k.

5. CyberRisk Quadrant[11]

Now it is time to start putting it all together.

1. Price

First, let's look at annual price, sorting products into high (large markers), medium (medium sized markers) and low categories (small markers). An *Annual Product Cost* (APC) less than $1000 is in the low category, an APC less than $5000 is in the medium category and all APCs above $5000 are in the high category. This leads to the following Table 3:

Vendor	Price	Complete Security Score vs. ROSI Graph Marker	Operational Efficiency Score vs. ROSI Graph Marker
AWS	Low		
Barracuda	High		
Cloudflare	Medium		
F5	High		
Fortinet	High		
Imperva	Medium		
Prophaze	Medium		
SiteLock	Low		
StackPath	Low		

Table 3. Product Pricing[12]

The round marker is used for the subsequent Figure 5 and Figure 7 graphs. The triangular marker is used for the subsequent Figure 6 and Figure 7 graphs. Because each product was evaluated in both categories, each product has both a circle and a triangle.

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

[11] All colors in figures and tables in this section are taken from vendor style guides and do not indicate quality.

[12] See appendix for additional details on pricing

2. COMPLETE SECURITY SCORE VS. ROSI

Second, the next thing to check is how the *Complete Security Score* relates to the Return On Security Investment (ROSI). This leads to the following graph. See Figure 5.

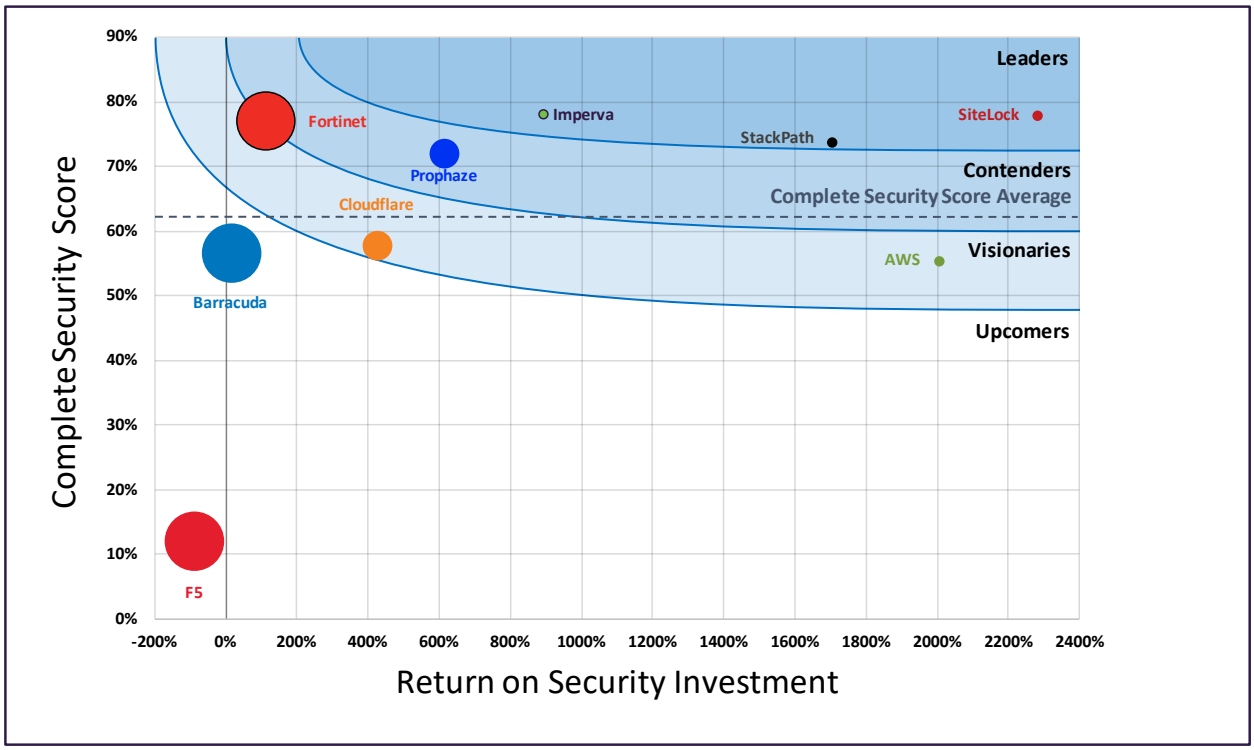

Figure 5. CyberRisk Security Efficacy Ripple

Four categories for Security Efficacy 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 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.*
  - Imperva, SiteLock and StackPath are *Security Efficacy Leaders*.
- ***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 zero and a *Complete Security Score* greater than one standard deviation below the average of the *Operational Efficiency* and *Security Efficacy Scores.*
  - Prophaze and Fortinet are *Security Efficacy Contenders*.
- ***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 negative of the average ROSI value and a *Complete Security Score* greater than two standard deviations below the average of the *Operational Efficiency* and *Security Efficacy Scores.*
  - AWS and Cloudflare are *Security Efficacy Visionaries.*

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

- ***Upcomers***: These Cloud WAF solutions demonstrated lower Security Efficacy standards which contributed to lower ROSI befitting small-to-medium enterprises and businesses. *Security Efficacy Upcomers* have a ROSI value less than the negative of the average ROSI value or a *Complete Security Score* less than two standard deviations below the average of the *Operational Efficiency* and *Security Efficacy Scores.*

  - F5 and Barracuda are *Security Efficacy Upcomers*[14].

The above figure also shows how the *Complete Security Score* (100% x SE) relates to ROSI. Equation 4 shows the minimum SE value to break even or attain a ROSI value of zero.

$$SE \geq APC \div ALE$$

Equation 4. Minimum SE Breakeven Calculation

3. Operational Efficiency Score vs. ROSI

Third, we look at the comparison 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.

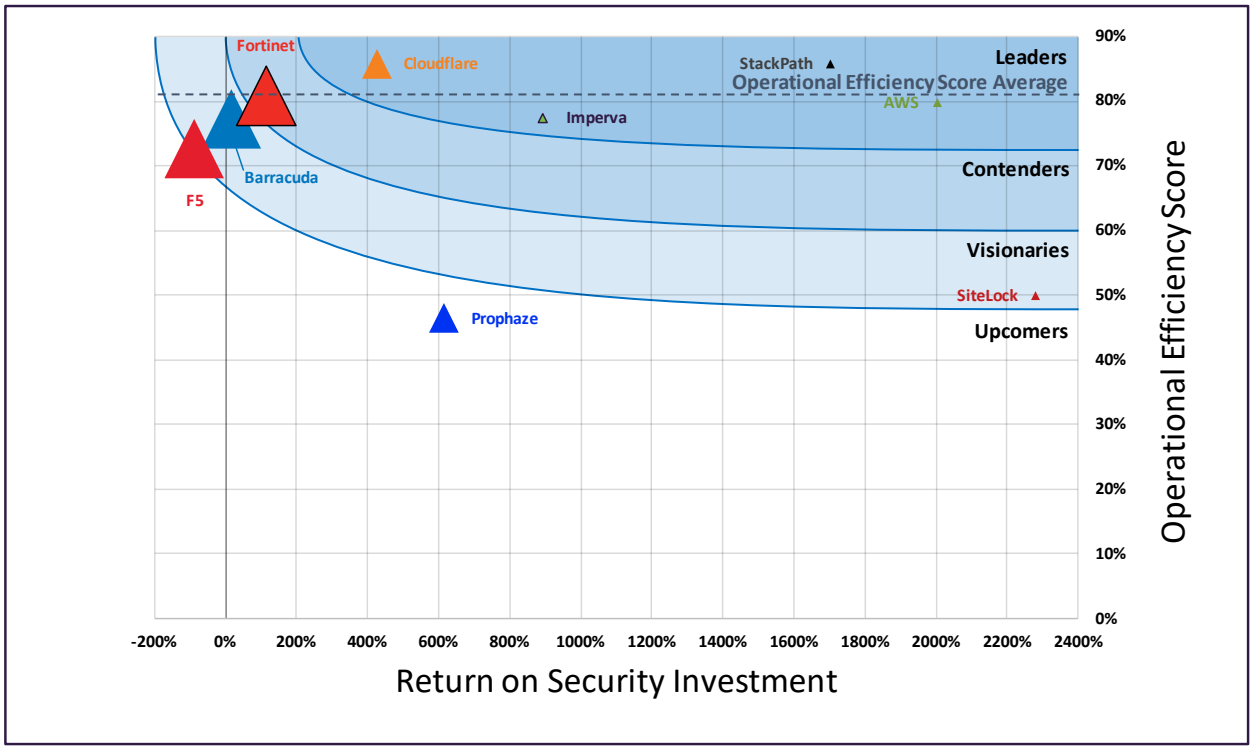

Figure 6. CyberRisk Operational Efficiency Ripple

Figure 6 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[15]. 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 a

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

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

Operational Efficiency Score greater than the average of the *Operational Efficiency* and *Security Efficacy Scores.*

- AWS, Cloudflare, Imperva and StackPath are *Operational Efficiency Leaders*.

- ***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, befitting to small-to-medium enterprises and businesses. *Operational Efficiency Contenders* have a ROSI value greater than zero and a *Operational Efficiency Score* greater than one standard deviation below the average of the *Operational Efficiency* and *Security Efficacy Scores.*
  - Fortinet 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 befitting small-to-medium enterprises and businesses. *Operational Efficiency Visionaries* have a ROSI value greater than the negative of the average ROSI value and a *Operational Efficiency Score* greater than two standard deviations below the average of the *Operational Efficiency* and *Security Efficacy Scores.*
  - Barracuda and SiteLock are *Operational Efficiency Visionaries*.
- ***Upcomers***: These Cloud WAF solutions demonstrated lower operational efficiency standards when it came to ease of deployment, integration and struck a poor balance between the technology and resource management, delivering a lower ROSI befitting small-to-medium enterprises and businesses. *Operational Efficiency Upcomers* have a ROSI value less than the negative of the average ROSI value or a *Operational Efficiency Score* less than two standard deviations below the average of the *Operational Efficiency* and *Security Efficacy Scores.*
  - F5 and Prophase are *Operational Efficiency Upcomers*[16].

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

4. SYNTHESIS

Assembling the previous data into one figure yields:

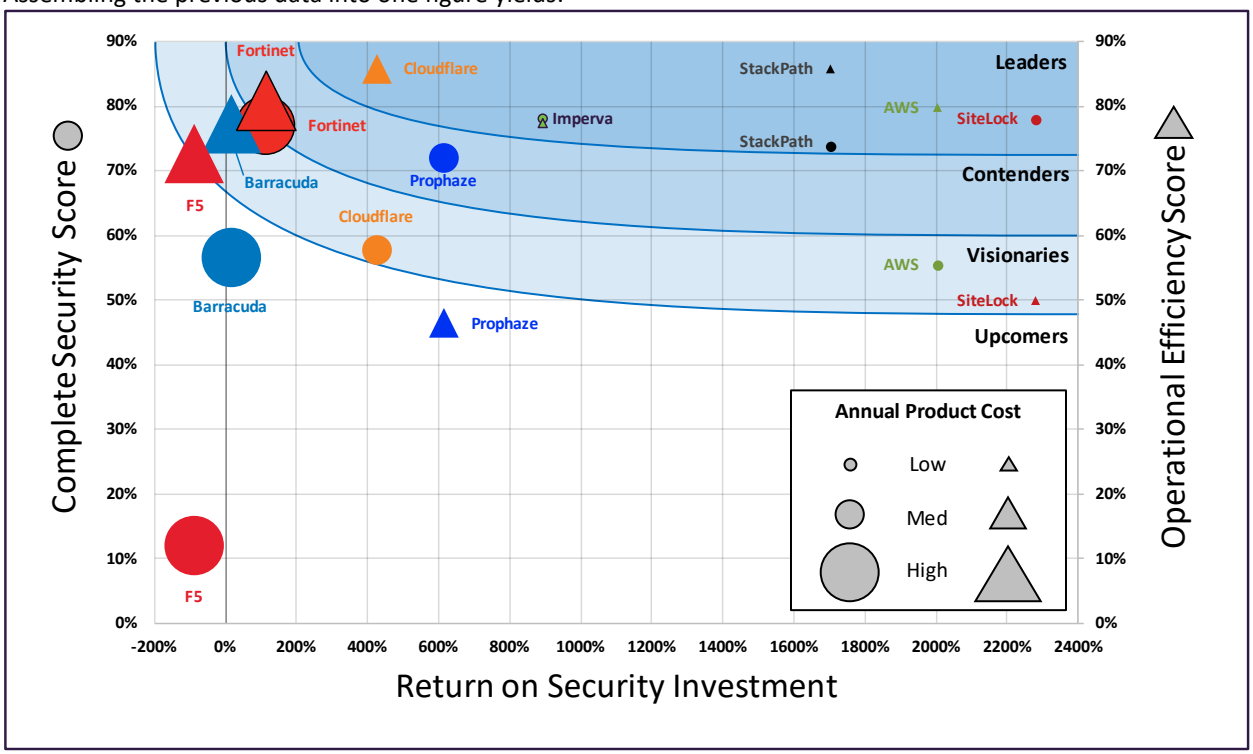

Figure 7. SecureIQLab Cloud WAF CyberRisk Ripple

The SecureIQLab Cloud WAF CyberRisk Ripple, Figure 7, is the culmination of an exhaustive and detailed approach to cloud WAF testing and validation research. This chart plots the Complete Security Score, circular markers, and the Operational Efficiency Score, triangular markers, versus ROSI. The upper right corner highlights the best operational efficiency, security efficacies and ROSI.

6. CONCLUSION

Summarizing the data from the previous section we get Table 4.

Vendor	Operational Efficiency	Security Efficacy
AWS	**Leader**	Visionary
Barracuda	Visionary	Upcomer
Cloudflare	**Leader**	Visionary
F5	Upcomer	Upcomer
Fortinet	**Contender**	**Contender**
Imperva	**Leader**	**Leader**
Prophaze	Upcomer	**Contender**
SiteLock	Visionary	**Leader**
StackPath	**Leader**	**Leader**

Table 4. SecureIQLab's Cloud WAF CyberRisk Ripple Results

By testing security efficacy and validating operational efficiency of popular cloud WAF solutions, that run the gamut from up-and-coming vendors to established vendors with deep roots in the security space, SecureIQLab supplies readers with a diversified starting point for consistency and how each security vendor is adapting and responding to the ever-changing threat landscape.

Apart from this comparative report which highlights the overall comparative metrics, SecureIQLab's individual test reports offer greater details for each of the venders tested. Still, given that every organization's attack surface, business requirements, and risk mitigation strategy are unique, thorough evaluation of cloud WAF technologies before deployment is recommended.

7. Appendix

1. Cloud WAF Test Deployment

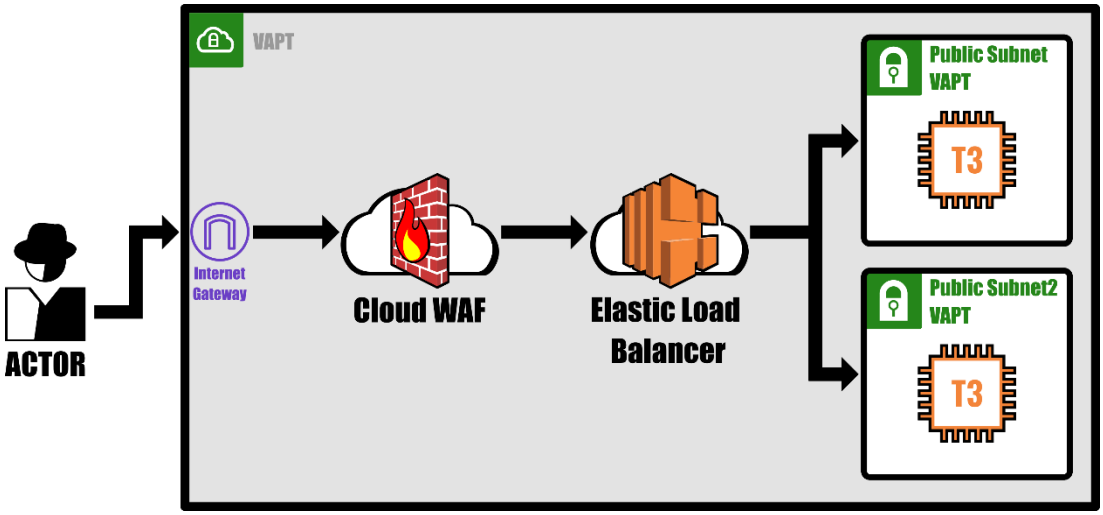

Figure 8. WAF deployment diagram

The cloud WAF was deployed with default policy with an elastic load balancer to protect the web-applications on AWS, see Figure 8. All web-application transactions were inspected by the cloud WAF. In doing so, the cloud WAF was expected to provide protections against threats that were originated by the malicious actors while allowing normal actors to access the web 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. See Table 6 for deployment findings.

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.

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 Fortinet's 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. More details on these techniques are covered in the Resiliency section.
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 PUT security effectiveness is measured.

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. Groups of exploits are carefully selected from this library to test based on the intended attack. Each exploit has been validated to impact the target vulnerable host(s) by compromising the asset, which can range from being the web server, the web application or sites. The level of compromise can vary between 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, browse and/or retrieve files stored on the host server, escalating user privileges, and so on.

4. Product Configuration

Cloud WAF products were deployed and configured according to the default instructions found on the vendors' websites and, where applicable, on AWS Marketplace.

5. Product Rules

Cloud WAF products were configured according to the default instructions found on the vendors' websites and, where applicable, on AWS Marketplace. Default rule sets were used for most 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.

5. Product Pricing[17]

Pricing for products tested are listed in Table 4. Product pricing models varied in simplicity, 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 nine vendors tested.[20] In order to best compare the variety of fruit tested, the pricing options used will be able to support up to:

- 5 GB monthly traffic
- 1 one million requests monthly
- 1 site being protected

Pricing was also calculated based on protection being on for entire month, fees are paid monthly, and protection against botnet attacks[21] is included.

Vendor	Yearly Subscription Cost
AWS	$540
Barracuda	$9,636
Cloudflare	$2,400
F5	$15,155
Fortinet	$7,446
Imperva	$1,560
Prophaze	$1,200
SiteLock	$420
StackPath	$900
Average	$4,362

Table 4. Pricing

[17] Support tiers and offerings vary by vendor and need to be considered for budgetary purposes. Support prices are not included in pricing table.
[18] Pricing will vary.
[19] Vendor standard feature sets may change with time.
[20] Pricing is dynamic. SecureIQLab noted pricing changes for at least three vendors during the testing period.
[21] Botnet protection is not a standard feature for all products.

8. Contact Information

SecureIQLab, LLC.

+1.512.575.3457

www.secureiqlab.com

info@secureiqlab.com

9. Copyright and Disclaimer

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

SecureIQLab (December 2021)