SecureIQlab™

Bridging the enterprise cloud security gap

Cloud Web Application Firewall (WAF) CyberRisk Validation Report – Prophaze Cloud WAF

Product Version: NA

Published: Sep 30th, 2021

Language: English

www.secureiqlab.com

Report Contents:

SecureIQlab™ Bridging the enterprise cloud security gap

1. INTRODUCTION

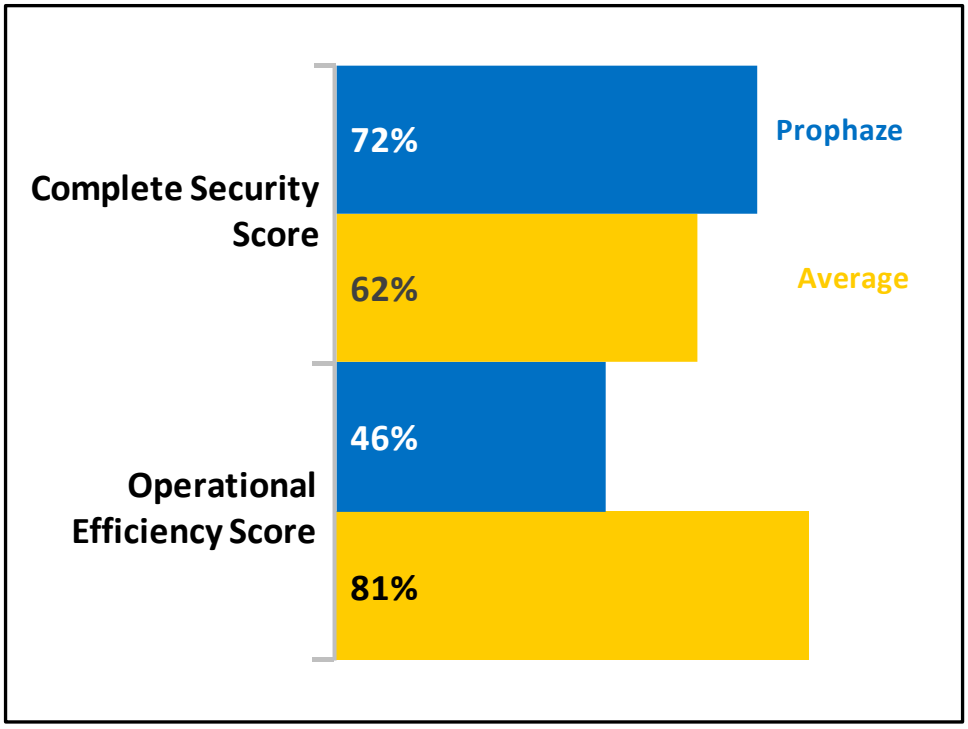

Figure 1. Overall Validation Results for Prophaze Cloud WAF

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 is not without challenges. There are risks associated with moving to the cloud. 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. The test was conducted in accordance with the standards of the Anti-Malware Testing Standards Organization[2] (AMTSO). The test used version 1.0 of the SecureIQLab Cloud WAF CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP039).

This report discusses the test results for the Prophaze Cloud WAF. To provide context, these individual results are presented alongside the collective averages for all nine of the tested products. This provides an at-a-glance comparative between the individual product under test and the collective results. One comparative report that highlights the performance of all nine vendors and individual reports for the remaining eight other tested WAF solutions are also available.

This CyberRisk Validation Report provides test results for the Prophaze Cloud WAF. Because thousands of attacks were simulated during the test, test results have necessarily been simplified and presented for review in a summary format for small and medium-sized businesses, enterprises, and managed service providers (MSPs). Figure 1 provides a summary of the product's overall validation results.

During the test, products were subjected to a battery of diverse attacks. Simple ecommerce applications and

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

multiuser web applications were used as targets. Empirically validated data based upon industry guidelines and regulations such as the OWASP Top 10[3] and PCI DSS[4] was obtained. It was obtained while securing targeted cloud applications on AWS with cloud WAFs.

SecureIQLab is an IT security 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.

Prophaze was founded in 2019 and is a key vendor in the WAF market. Prophase's WAF was selected for inclusion in this test because it meets the SecureIQLab WAF validation methodology selection criteria.[6]

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 Prophaze Cloud WAF 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 Prophaze website and according to relevant documentation available on Prophaze's documentation site 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, i.e., SMBs, managed service providers (MSPs), and managed security service providers (MSSPs). Tuning a WAF can be complex. Enterprises are advised to exercise due diligence 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.

[3] Open Web Application Security Project®

[4] Payment Card Industry Security Standards Council

[5] https://owasp.org/

[6] Analyst and Enterprise Challengers - Small-mid-large enterprise security professional surveys, direct 1:1 inquiries and engagement with enterprises, organizations, MSP's, MSSP's, Gartner MQ, buyers guide, and Forrester Wave.

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 Result Overview

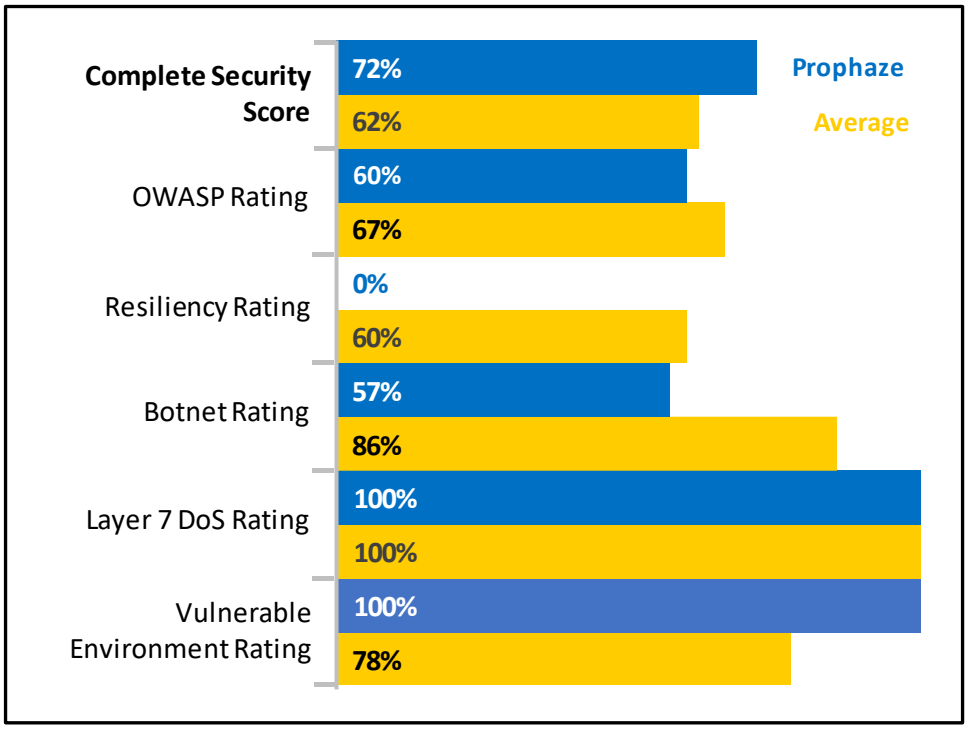

Figure 2. Security Validation Results for Prophaze Cloud WAF

Figure 2 above provides an overview of the SecureIQLab findings during security validation of the Prophaze WAF. 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. The calculation method 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.

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

Equation 1. Calculation of Complete Security Score

Every cloud WAF evaluated in this test was subjected to twelve different categories of 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. OWASP Rating[7]

The Open Web Application Security Project (OWASP) is a non-profit foundation dedicated to improving web

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

application security[8]. The OWASP Top 10[9] Report is assembled by security experts from across the globe and describes the most critical web application vulnerabilities.

The Prophaze Cloud WAF was tested against five of these vulnerabilities. SecureIQLab selected these vulnerabilities based on vulnerability prevalence and operational requirements.[10]

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

OWASP	OWASP Vulnerbility Critical Rating				Test Results for Prophaze			
	Exploitability	Prevelance	Detectability	Technical	# Attacks	# Blocked Attacks	% Blocked	Test Average
Injection Vulnerabilities	3	2	3	3	-	-	90%	46%
SQL Injection					2225	1926	87%	59%
Command Injection					2659	2321	87%	28%
CRLF Injection					78	72	92%	36%
HTML Injection					5	5	100%	18%
Host Header Injection					8	8	100%	56%
Server Side Template Injection					140	124	89%	29%
LDAP Injection					45	45	100%	100%
Xpath Injection					16	11	69%	44%
XML External Entities (XXE) Vulnerabilities	2	2	3	3	-	-	0%	64%
Unrestricted File upload					4	0	0%	75%
XML External Entity Attacks					105	0	0%	52%
Cross-Site Scripting XSS Vulnerabilities	3	3	3	2	10209	10078	99%	86%
Broken Access Control Vulnerabilities	2	2	2	3	-	-	11%	43%
Path Traversal					6951	1580	23%	42%
Brute Force					1	0	0%	44%
Sufficient Logging & Monitoring	2	3	1	2	NA	NA	100%	89%
OWASP Rating							**60%**	**67%**

Table 1. OWASP Vulnerability Validation

Category averages are determined by equally weighting the test case averages within each category. As an example, Equation 2 below provides the formula for calculating the average for the *Broken Access Control Vulnerabilities* category.

Broken Access Control Vulnerabilities = [Path Traversal + Brute Force]/2

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

In addition to security efficacy, the product's logging and monitoring capabilities were reviewed. More detailed analysis of these capabilities may be found in Section 3 under *Logging, Monitoring, and Auditing.*

3. Resiliency Rating

Security products must demonstrate resiliency. Failure to do so will have significant consequences. 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."[11]

To test its operational resilience, The Prophaze Cloud WAF was tested against several attack masking techniques to determine whether it could successfully block attacks that would otherwise go unseen. A higher resiliency rating indicates a product is more capable of withstanding and absorbing different variations of attacks while a lower

[8] SecureIQLab is not affiliated with OWASP.

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

[10] Testing a product against all 10 categories may yield different overall results.

[11] https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodi/850001_2014.pdf#page=57

resiliency rating indicates a product is less likely to detect different variations of attacks.

Five test cases were employed to test the resiliency of the Prophaze Cloud WAF. Table 2 below provides the test cases and the product's results. The *Resiliency Rating* is calculated by averaging the results of the five test cases.

Resiliency	Test Results for Prophaze	
	Blocked/Bypassed	Test Average
Web Shell Attack	0%	67%
Custom Web Shell Attack	0%	33%
Out-of-Band Data Exfiltration	0%	67%
SQL Injection WAF Ruleset Evasion	0%	67%
Command Injection WAF Ruleset Evasion	0%	67%
Resiliency Rating	**0%**	**60%**

Table 2. Resiliency Validation Results

4. Botnet Attacks

A botnet is a network of compromised computers that is used by a remote administrator to carry out automated attacks. Prophaze Cloud WAF was tested against seven types of bot attack. 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 (see Table 3 below). The *Botnet Rating* is calculated by averaging the seven contributing scores.

BOTNET Attacks	Test Results for Prophaze	
	Blocked/Bypassed	Test Average
Credential Stuffing Attack	0%	56%
Tor-Based Layer 7 Attack	100%	100%
Web Content Scraping	0%	89%
Form Submission Abuse Attack	0%	56%
Website Crawler	100%	100%
Broken Link Checker	100%	100%
Bot User Agent Attack	100%	100%
Botnet Rating	**57%**	**86%**

Table 3. Botnet Attack Results

5. Layer 7 DoS Attacks

Layer 7 denial-of-service (DoS) attacks are more difficult to detect than other DoS layer attacks because they use a valid TCP connection. Test cases for such attacks are also more infrastructure friendly than distributed denial-of-service (DDoS) attacks and thus avoid the issues that DDoS attacks may trigger with cloud service providers. Below, Table 4 presents the results of testing the Prophaze Cloud WAF against five Layer 7 DoS attacks. The product's *Layer 7 DoS Rating* was determined by taking the average of its scores against the five attacks

Layer 7 DoS	Test Results for Prophaze	
	Blocked/Bypassed	Test Average
HTTP Flood Attack	100%	100%
Asymmetric Attacks	100%	100%
Repeated Single Attacks	100%	100%
Application-Exploit Attacks DoS	100%	100%
Slowloris DDoS Attack	100%	100%
Layer 7 DoS Rating	**100%**	**100%**

Table 4. Layer 7 DoS Validation

6. Web Application Protection

A cloud-based WAF should protect vulnerable web applications. While the proliferation of web application frameworks has made deployment and maintenance of web applications simpler, it has also made it challenging to update these frameworks without affecting the functionality of the web applications. Businesses, and MSSPs by extension, can ill afford downtime and may delay updates to avoid breaking applications. Consequently, WAFs can remain vulnerable to various published vulnerabilities and exploits, which makes it easier for cybercriminals and script kiddies to compromise applications.

The Prophaze WAF was tested against non-zero-day exploits and successfully blocked all attacks. See Table 5 below for the full results. The *Vulnerable Web Environment Rating* is calculated by taking the average of the three vulnerability scores.

Vulnerable Web Environment	Test Results for Prophaze	
	Blocked/Bypassed	Test Average
Vulnerable Wordpress Installation	100%	78%
Vulnerable Joomla Installation	100%	78%
Vulnerable Drupal Installation	100%	78%
Vul. Web Env. Rating	**100%**	**78%**

Table 5. Vulnerable Web Environment Results

3. Operational Efficiency

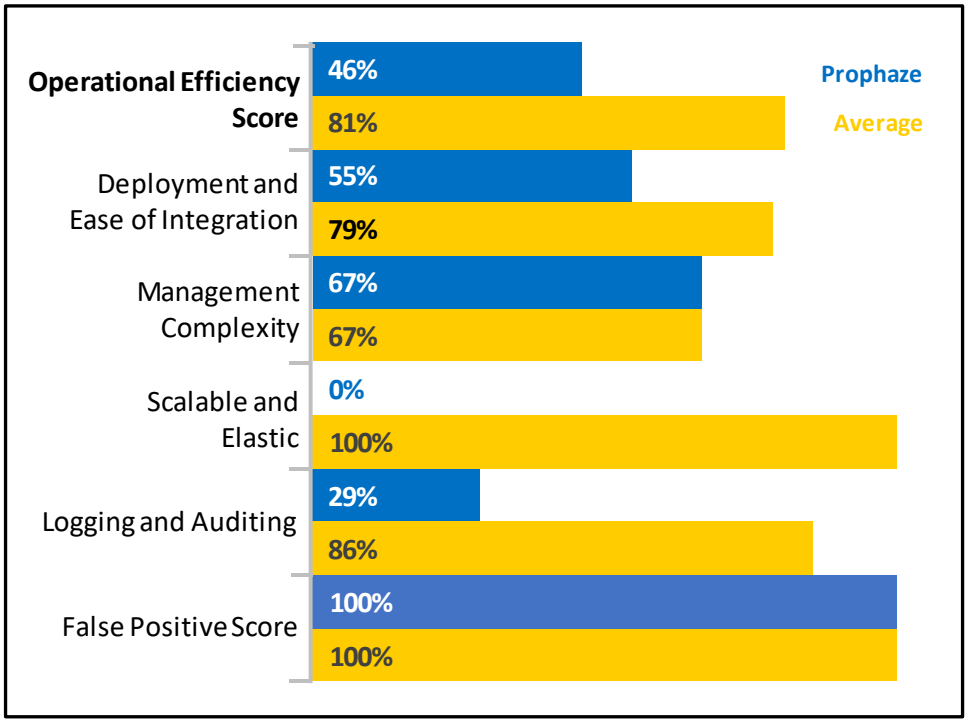

Figure 3. Validation of Operational Efficiency for Prophaze Cloud WAF

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

Prophaze Cloud WAF was validated in each of these areas of operational efficiency. Figure 3, above, displays the product's high-level results.

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.

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 3 states the *Operational Efficiency Score* calculation.

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

Equation 3. 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.*

7. Deployment and Ease of Integration

Cloud WAFs typically take less than an hour to a few days to set up and seldom require installation of software or hardware.

Cloud WAFs should integrate with other security tools, Security Information and Event Management (SIEM) systems, and data repositories. This typically allows both tasks and alerts to be automated. Typical integrations include DevOps tools like Slack and Jira and can include automated additions to policies as threats are detected.

SecureIQLab validated the ease of deployment and integration for the Prophaze Cloud WAF. Prophaze Cloud WAF comes as an SaaS (Software as a Service) and can be managed via Web UI. A minimal understanding of AWS resources is a prerequisite to deploy. Findings for deployment and ease of integration are in Table 6 below.

Deployment and Ease of Integration	Validation Results	
	Prophaze Results	Test Average
Time to Deploy	0 minutes	29 minutes
# of Steps for Setting Up WAF Service	1 step	3 steps
# of Steps for Requesting a Public Certificate	NA	2 steps
# of Steps for Requesting a Private Certificate	NA	3 steps
# of Steps to Add an SSL Certificate to an Existing Site	NA	3 steps
Application Load Balancing and Monitoring	NA	Yes
Integration with Multi-Cloud WAF	Yes	NA
Plug and Play Integration with On-prem Firewall	Yes	NA
Plug and Play Integration for SIEM/S3 Bucket	Yes	Yes
Plug and Play Integration for API Gateway	NA	Yes
Required Contacting Support During Deployment	No	No

Table 6. Deployment and Ease of Integration Findings

The *Deployment and Ease of Integration Score* is the percentage of the Prophaze WAF 30 points earned to the possible 33 points, or 91%. The group score average for *Deployment and Ease of Integration* was 79%.

8. Management Complexity

Cloud WAFs market the promise that they are more easily managed than on-premises solutions. They are less complex and more easily managed because they receive automated updates, automatically deal with spikes in traffic (as discussed below) and work out of the box.

Cloud WAFs are less complex because the cloud WAF provider manages the security details and automatically allocates the resources needed. The cloud WAF provider typically has already tuned the security software. Users typically have a single management console to monitor.

Users can typically create additional policies that allow identity-based access and network segmentation. Because the cloud WAF provider automatically applies policy modifications wherever the cloud WAF is deployed, policy modification is generally simple and rapid. Results from SecureIQLab's experience while managing Prophaze Cloud's WAF are in Table 7, below.

Management Complexity	Validation Results	
	Prophaze Results	Test Average
Complexity of Tuning WAF	Low	Low
Complexity of Setting Security Policy	Low	Low
Complexity for Setting Up WAF	Low	Low
Managing WAF Updates	Automatic	Automatic
Complexity of Managing Web ACL	NA	NA
Internal WAF Migration Complexity	NA	NA

Table 7. Management Complexity Experience

The *Management and Complexity Score* is the percentage of earned points for Prophase Cloud WAF, 12, to the total complexity points possible, 18 points or 67%. The group score average for *Management Complexity* was 67%.

9. Scalable and Elastic

Cloud WAFs should help the customer avoid sizing issues planning by providing for automated flexible scaling. Scaling typically occurs in response to changing traffic load patterns. Providers typically allow customers to choose options that balance optimizing performance and optimizing costs. Table 8 highlights SecureIQLab's findings in this area.

Scalable and Elastic	Validation Results	
	Prophaze Results	Test Average
Auto-Scaling Capability	NA	Yes
Manual Scaling Capability	NA	Yes
Load Balancing and Failover	NA	Yes

Table 8. Scalable and Elastic Validation

The *Scalable and Elastic Score* is the percentage of the earned 9 points by Prophaze to the total possible 9 points or 100%. The group score average for *Scalable and Elastic* was 100%.

10. Logging, Monitoring, and Auditing

Sufficient logging capabilities are required for incident response, auditing, and many compliance and regulatory purposes. Cloud WAFs need to provide enough visibility into web traffic and sufficient control capabilities for security teams to spot issues and resolve them. Additionally, Cloud WAFs need to have a means to integrate logged data with other storage devices for redundancy. Below, Table 9 covers our logging, compliance and auditing

findings.

Our researchers found that setting up logs was a one-step process to configure logs. Logs are available in CSV and Text format. There are at least 8 default dashboards for analytics.

Logging and Auditing	Validation Results	
	Prophaze Results	Test Average
Log Configuration Complexity	Low	Low
Third Party Log Storage Facility	NA	Yes
Web Request Inspection	Yes	Yes
Multi-Factor Authentication	NA	Yes
Application Monitoring	NA	NA
Infrastructure Monitoring	NA	Yes
# Audit Trail Fields	NA	7 fields

Table 9. Log and Audit details

The *Logging and Auditing Score* is the percentage of the 18 points earned by the Prophaze WAF to the total 21 total possible points for this section or 86%. The group score average for *Logging and Auditing* was 86%.

11. Allows Good Transactions – False Positives

WAFs need to allow for business-related transactions while blocking malicious activity. The false positive rate is important because false positives prevent the operation of the business. Policies need to be adjusted to minimize false positives.

False Positives increase noise for already stretched thin security teams and contribute to alert fatigue. Properly tuned security devices will not improperly detect benign traffic as malicious. Four different false positive test cases were used to validate that the WAF under test would not block simulated consumer purchases. These test cases simulated users that would browse the web application normally while being protected by the cloud WAF. Given the importance of WAFs not interfering with ecommerce, all four test cases are required to pass through the product under test to receive a passing score. The results for the false positive testing are found below in Table 10. *The False Positive Score* is the percentage of the 3 points earned by Prophaze to the total possible 3 points. The higher the *False Positive Score*, the lesser the operational overhead in tuning the WAF.

False Positives	Test Results	
	Prophaze False Positive Results	Group False Positive Results
False Positive Tests	100%	100%
False Positive Score	**100%**	**100%**

Table 10. False Positive Testing Results

4. APPENDIX

1. CLOUD WAF TEST DEPLOYMENT

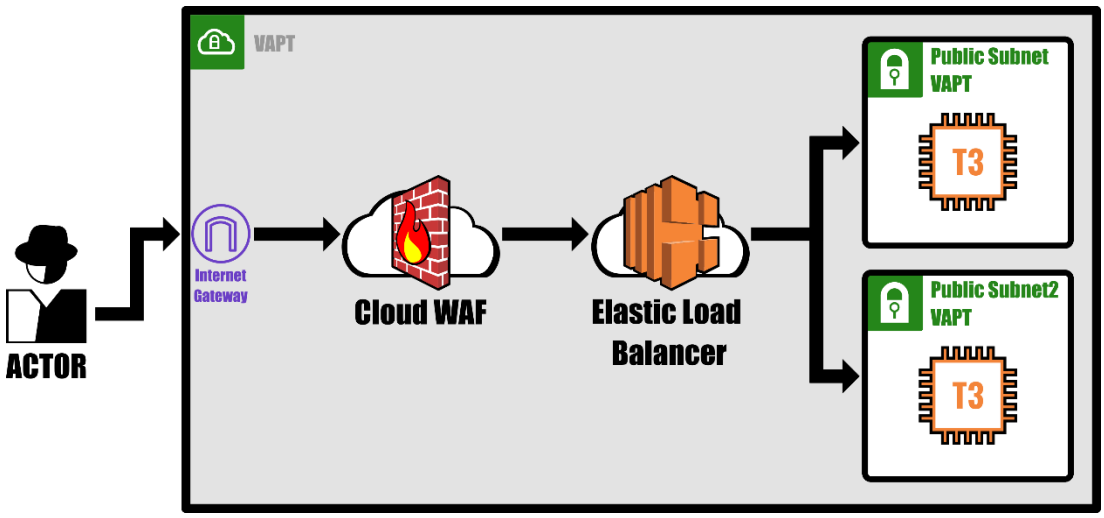

Figure 4. WAF deployment diagram

The cloud WAF was deployed with default policy with an elastic load balancer to protect the web-applications on AWS, see Figure 4. 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 Prophaze'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. Prophaze Cloud WAF Configuration

The Prophaze Cloud WAF was deployed and configured according to the default instructions found in the Prophaze

Documentation site[12].

5. PROPHAZE CLOUD WAF RULES:

The Prophaze Cloud WAF was configured per Prophaze's default configuration.

5. CONTACT INFORMATION

SecureIQLab, LLC.

801 Barton Springs Road

9th Floor

Austin, TX 78704 USA

+1.512.575.3457

www.secureiqlab.com

info@secureiqlab.com

6. COPYRIGHT AND DISCLAIMER

[12] https://docs.prophaze.com/