SecureIQlab®

REPORT

CyberRisk Validation Report – Amazon

Product Version: Amazon AWS Network Firewall

Published: 22 March 2024

Report Contents

1. Introduction

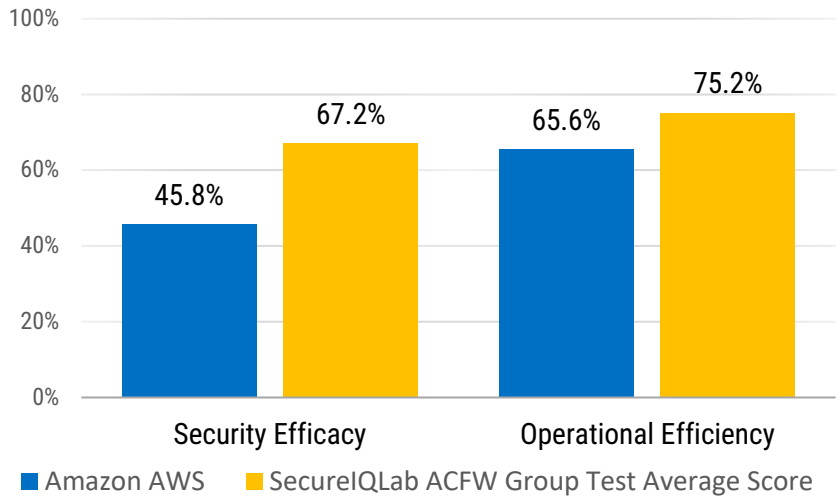

Figure 1. Summary Results for Amazon vs the ACFW Group Test Scores

Advanced Cloud Firewalls (ACFW) protect the infrastructure that organizations depend on. These firewalls serve as a virtual shield. ACFWs use a proactive approach and are designed to simplify security.

SecureIQLab conducted testing for 12[1] leading enterprise-class ACFW solutions. This test was conducted in accordance with the Anti-Malware Testing Standards Organization[2] (AMTSO) test Standard. The maps to version v1.6 of the SecureIQLab Advanced Cloud Firewall CyberRisk Validation Methodology, AMTSO Test ID: AMTSO-LS1-TP070. It is the most comprehensive evaluation of its kind ever performed.

As part of this test, SecureIQLab completed testing Amazon AWS Network Firewall. This report discusses the test results for the Amazon AWS Network Firewall.

This report offers empirical data points on what to expect from the Amazon AWS Network Firewall, highlighting features and business considerations. SecureIQLab's testing showcases the overall organizational value of the Amazon AWS Network Firewall in security effectiveness and operational efficiency. Figure 1 highlights Amazon's results in these two areas versus the group test averages.

As Figure 1 shows visually, Amazon AWS Network Firewall results were below the average ACFW tested.

In writing this report, SecureIQLab has made extensive efforts to guarantee the accuracy of the results while straightforwardly presenting them. However, the test results are necessarily simplified to be presented for review in a summary format.

[1] Testing was attempted on a total of 12 Advanced Cloud Firewall solutions. Please click here for details.
[2] Standards https://www.amtso.org/ conducted testing.

2. Report Summary

This 2024 Advanced Cloud Firewall CyberRisk Validation Report provides test results for the Amazon AWS Network Firewall. Table 1 summarizes the product's overall validation results around security effectiveness, resistance to false positives, operational efficiency, and SSL/TLS security efficacy of the Amazon AWS Network Firewall solution validated against SecureIQLab ACFW v1.6 methodology.

ACFW Test Categories	Amazon ACFW Score	SecureIQLab ACFW Group Test Average Score
Security Efficacy	45.8%	67.2%
Resistance to False Positives	98.7%	89.8%
Operational Efficiency	65.6%	75.2%
SSL/TLS Security Efficacy	Contact SecureIQLab	68.4%

Table 1. Amazon ACFW Result Summary

Figure 2 presents the above table in visual format.

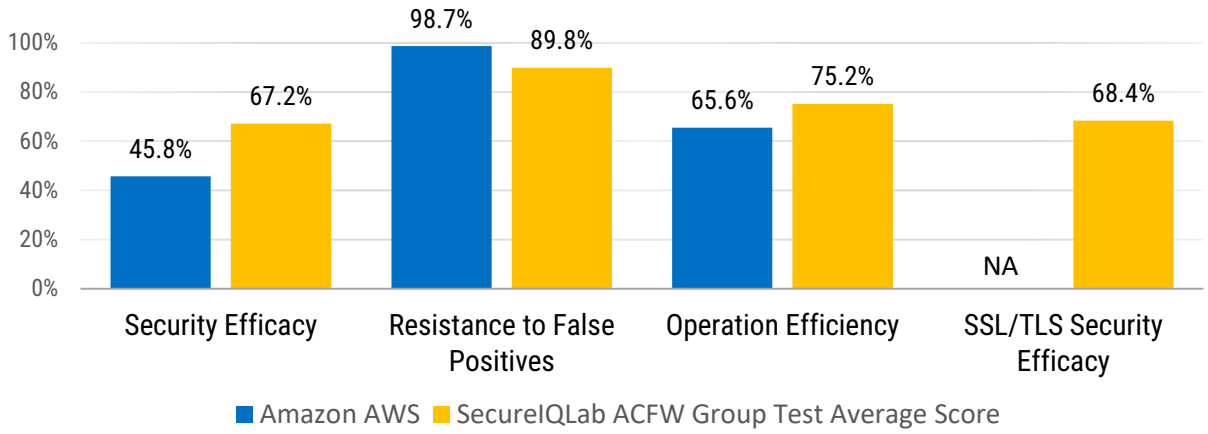

Figure 2. Overall Result Summary: Amazon ACFW vs SecureIQLab ACFW Group Test Average

Overall Result Summary: Amazon AWS Network Firewall did well compared to the overall SecureIQLab ACFW group test average in one of the primary enterprise categories as represented in the SecureIQLab ACFW validation methodology selection criteria.[3]

[3] SecureIQLab ACFW v1.6 methodology

3. ACFW Test Overview

Advanced Cloud Firewalls (ACFWs) must effectively counter the emergence of advanced attack vectors, novel strategies, and new attack surfaces, thwarting threats that are complex and customized. Beyond merely being aware of application use of the internet, they should possess capabilities to inspect packet content and search for Indicators of Attack (IOA) within the data stream. This test was designed to confirm how well the tested ACFW was able to:

- Identify permitted applications and block prohibited applications.
- Identify and block threats attempting to use “known good” ports and protocols.
- Identify and block threats that attempt evasive tactics, such as non-standard ports or “port hopping.”
- Identify and block threats encrypted with SSL/TLS.
- Identify users, groups, and locations, and apply policy regardless of I.P. address.
- Identify and block outbound data leaks.
- Identify and block outbound Botnet Command and Control communications.
- Enable secure business workflow with a high detection rate and low Signal-to-Noise ratio.
- Provide global visibility and granular policy management.
- Provide all necessary alerts and configuration recommendations based on best practices.

SecureIQLab defines prevention as a 24/7 automated response offering without human intervention. This can be achieved through various technologies and mechanisms, including signature-based models, policy-based models, behavior-based models, and machine learning (ML) or artificial intelligence (AI)-based models. This definition is technology-agnostic, focusing on outcomes of the various analyst workflows and scenarios rather than the specific prevention technology. ACFWs, when deployed in a stand-alone mode, are expected to prevent both initial and ongoing attacks while also providing robust reporting capabilities.

The SecureIQLab ACFW v1.6 validation methodology was tailored towards the prevention and reporting capabilities for security and compliance. Configurations typically included multiple security and compliance applications such as Vulnerability Protection, Anti-Spyware, Antivirus, URL Filtering, and DNS Security. By default, when configuring, “detect” settings were set to "protect" or "block". SecureIQLab then performed any required tuning according to recommended vendor best practices for operational scenarios involving cloud deployments[4].

3.1 ACFW Deployment Overview

Per SecureIQLab's methodology, all ACFW vendors were requested to configure their products based on best practices that enterprises should implement when deploying the firewall in their organizations. The intent of this testing methodology is to mirror a successful customer experience during the deployment and management of the product.

During the evaluation, SecureIQLab ensured product updates and configuration changes were executed through a central management console: cloud or on-prem device portal. This approach aimed to cover all test scenarios from start to finish to the greatest extent possible.

For a more comprehensive understanding of our testing methods, refer to version 1.6 of the SecureIQLab 2023 ACFW CyberRisk Validation Methodology (AMTSO Test ID: AMTSO-LS1-TP070).

[4] AWS Network Firewall deployment reference.

4. Security Efficacy Results

Advanced Cloud firewalls should be designed to protect cloud-based resources and applications, shielding them from unauthorized access and prevalent cyber threats.

Each ACFW solution evaluated in this test underwent scrutiny across multiple distinct enterprise-centric categories, involving attack vectors of more than 1000 real-world operational scenarios. These scenarios used real world attacks that have targeted small-to-medium size businesses, enterprises, and other organizations. The comprehensive testing performed by SecureIQLab reflects our commitment to innovation and continuous improvement. Moving forward, SecureIQLab plans to continue to augment attack libraries and incorporate additional relevant operational metrics as needed in future iterations of this test.

The Amazon AWS Network Firewall was tested against 13 attack types within four primary standard threat categories. Table 2 below presents the results of these tests. Figure 3 below presents an overview of the SecureIQLab findings during the security effectiveness validation and reporting of the Amazon AWS Network Firewall. This includes the standard threat category score, the advanced threat category score, the operational accuracy score, and the SSL/TLS threat efficacy score from the methodology. These sections of the methodology were selected for presentation because these sections tested each ACFW against the four primary standard threat categories.

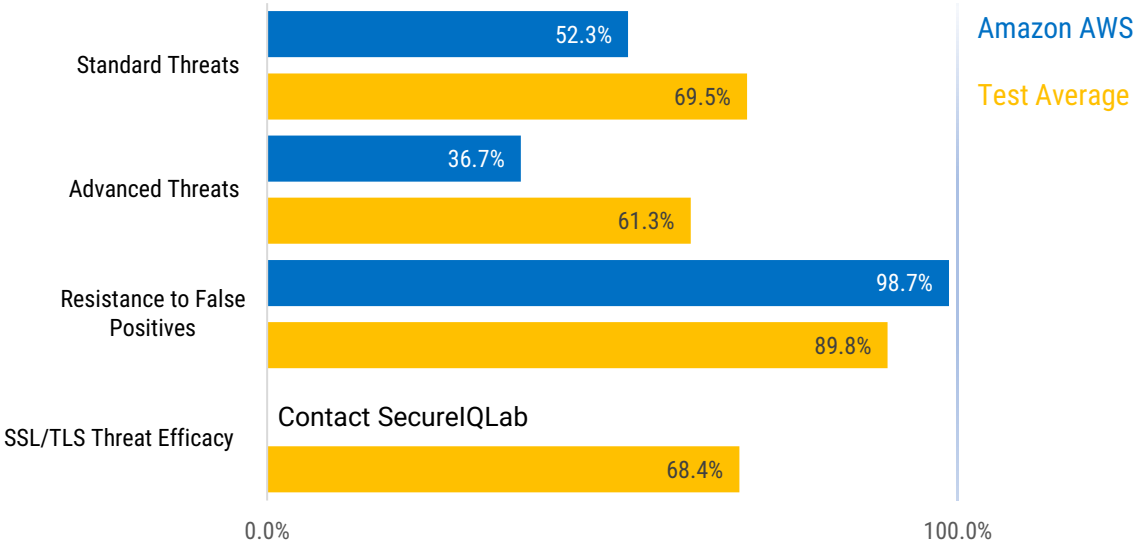

Figure 3. Amazon Advanced Cloud Firewall Security Effectiveness

4.1 Common Cloud Firewall Threat Categories (Standard Threats)

The Common Cloud Firewall Threat (Standard Threats) average scores are calculated by averaging the scores for each threat type together within their respective attack category.

Standard Threat Types	Amazon ACFW Inspection Score	SecureIQLab ACFW Group Test Average Score
Application-Based Threats		
Cross-Site Scripting (XSS) Attacks – HTTP	100.0%	75.5%
Cross-Site Scripting (XSS) Attacks – HTTPS	100.0%	67.1%
Malicious URL Attacks	5.7%	68.0%
Malware & Botnets		
Malware Download over HTTPS	Contact SecureIQLab	61.3%
Compressed Malicious Files	Contact SecureIQLab	60.2%
Botnets	23.7%	58.3%
Browser-Based Threats		
Browser Exploits	100.0%	74.0%
Cookie Stealing - HTTP	100.0%	85.0%
Cookie Stealing - HTTPS	100.0%	100.0%
Browser Version and Plugin-in Control	50.0%	60.0%
Obfuscated JavaScript	100.0%	90.0%
Data-loss and Leakage		
Phishing Site-Based Attacks	Contact SecureIQLab	56.6%
Adware Site Prevention	FAIL	PASS
Standard Threats Average Score	52.3%	69.5%

Table 2. Standard Threats Protection Testing

The Amazon ACFW scored 100% in six of the thirteen attack categories.

4.2 Advanced Cloud Firewall Threat Categories

Advanced Cloud firewalls must extend their protective capabilities to counter advanced threats, which are often sophisticated, highly evolved, and challenging to detect or neutralize. Such threats may employ various tactics and techniques to circumvent traditional security measures. As a pivotal component of any organization's cybersecurity infrastructure, a robust cloud firewall should possess threat detection capabilities, be able to identify suspicious network traffic patterns and have the capacity to block in real time.

The Amazon AWS Network Firewall was tested against eight attack types classified as advanced threats. Table 3 below provides the results from these tests.

Advanced Threat Classification	Amazon ACFW Inspection Score	SecureIQLab ACFW Group Test Average Score
Advanced Evasive Techniques (Application-based)	38.0%	79.6%
Advanced Evasive Techniques (Network-based)	100.0%	75.0%
Known Malicious Files	Contact SecureIQLab	60.2%
Malicious Documents	Contact SecureIQLab	59.3%
Active Cloud-Based Threats (aka Active Threats)	5.9%	46.5%
Advanced Persistent Threats (APT)	Contact SecureIQLab	65.0%
Cloud-Centric Post Exploitation Techniques (Post-Exploitation – DNS Tunnelling)	100.0%	45.0%
Cloud-Centric Post Exploitation Techniques (Post-Exploitation – ICMP Tunnelling)	50.0%	60.0%
Advanced Threats Average Score	36.7%	61.3%

Table 3. Advanced (Non-Standard) Threat Protection Testing

The Advanced Cloud Firewall Threat average scores are calculated by averaging the scores for each threat type together within their respective attack category. Amazon performed better than average with a score of 100.0% in Network-based Advanced Evasive Techniques.

4.3 Operational Accuracy Category

False positive testing was included in the scope of this test because an Advanced Cloud Firewall that prevents 100% of malicious attacks but also prevents legitimate (non-malicious) actions can be vastly

disruptive. SecureIQLab used appropriate tools and techniques to ensure that the tested firewall products do not generate significant numbers of alerts with legitimate applications and processes in an enterprise environment. This section of the methodology was performed at the same time as and as part of the validation workflow and other independent sections wherever feasible. The aim is to ensure that the firewall products did not prevent malicious traffic at the expense of operational accuracy.

The Amazon AWS Network Firewall was tested for operational accuracy under real-world scenarios during the entire test cycle, and Table 4 below provides the results from these tests.

Operational Accuracy test	Amazon ACFW Score	SecureIQLab ACFW Group Test Average Score
Resistance to False Positive Test	**98.7%**	**89.8%**

Table 4. Operational Accuracy

The Amazon AWS Network Firewall performed above average in this test.

4.4 ACFW SSL/TLS Support

Hypertext Transfer Protocol (HTTP) and its secure analogue HTTPS have long been crucial internet protocols. HTTPS uses encryption to enhance browsing safety by establishing secure connections between browsers, applications, and websites. To identify the attacks or threats in encrypted connections, the firewall must inspect the encrypted traffic using SSL/TLS ciphers and the associated techniques for managing encrypted connections. To detect a threat concealed within encrypted data, the firewall must decrypt packets, inspect the content, and take necessary action.

For each ACFW tested, SecureIQLab tested 22 of the TLS v1.2 ciphers and 3 TLS v1.3 ciphers. The testing included combinations of ciphers between clients and servers to analyze firewall behavior with weak ciphers, to assess how the firewall behaved to communication using different ciphers, and to evaluate the ACFW's ability to fall back or enforce secure ciphers during communication.

The Amazon AWS Network Firewall was tested for overall SSL/TLS threat efficacy and its ability to protect against attacks delivered through the supported ciphers in real-world scenarios. Please contact SecureIQLab regarding the Amazon ACFW performance during the SSL/TLS test cycle. Table 5 below presents the results of these tests.

SSL/TLS Threat Efficacy Test	Amazon ACFW Overall Metric	SecureIQLab ACFW Group Test Average Score
Overall SSL/TLS Security Efficacy	Contact SecureIQLab	**68.4%**

Table 5. SSL/TLS Threat Efficacy

The cipher suites for TLS v1.2, as highlighted in Table 6 below, were tested for the Amazon AWS Network Firewall.

TLSv1.2 Ciphers	TLS Support	TLS Handshake Result	Attack Traffic Prevention within TLS Session	Operational Validation with Operational TLS Traffic
AES128-GCM-SHA256	Contact SecureIQLab			
AES128-SHA				
AES256-GCM-SHA384				
AES256-SHA				
AES256-SHA256				
DHE-RSA-AES128-SHA				
DHE-RSA-AES256-SHA				
DHE-RSA-AES256-SHA256				
DHE-RSA-CHACHA20-POLY1305				
ECDHE-ECDSA-AES128-GCM-SHA256				
ECDHE-ECDSA-AES128-SHA				
ECDHE-ECDSA-AES128-SHA256				
ECDHE-ECDSA-AES256-GCM-SHA384				
ECDHE-ECDSA-AES256-SHA384				
ECDHE-ECDSA-CHACHA20-POLY1305				
ECDHE-RSA-AES128-GCM-SHA256				
ECDHE-RSA-AES128-SHA				
ECDHE-RSA-AES128-SHA256				
ECDHE-RSA-AES256-GCM-SHA384				
ECDHE-RSA-AES256-SHA				
ECDHE-RSA-AES256-SHA384				
ECDHE-RSA-CHACHA20-POLY1305				

Table 6. TLS v1.2 Cipher Support

Contact SecureIQLab regarding AWS Network Firewall's TLS v1.2 cipher support.

The cipher suites for TLS v1.3, as highlighted in Table 7 below, were tested for the Amazon AWS Network Firewall.

TLSv1.3 Ciphers	TLS Support	TLS Handshake Result	Attack Traffic Prevention within TLS Session	Operational Validation with Operational TLS Traffic
AES256-GCM-SHA384	Contact SecureIQLab			
CHACHA20-POLY1305-SHA256				
AES128-GCM-SHA256				

Table 7. TLS v1.3 Cipher Support

Contact SecureIQLab regarding AWS Network Firewall's TLS v1.3 cipher support.

5. Security Resiliency Results

Security products must demonstrate overall resiliency, as failure to do so can have significant consequences. The Department of Defense (DoD) defines security resilience as *"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."*

SecureIQLab has adopted a novel approach to define the firewall resiliency metrics. Our security resiliency rating combines security efficacy with key operational and cloud-based performance metrics based on a real-world scenario. This holistic approach considers the firewall's security efficacy (threat protection) and operational efficiency metrics mapped to crucial capabilities and ACFW workflows relevant to enterprise use cases subjected to real-world traffic.

The security resiliency test used a simulated real-world cloud-based traffic mix. The traffic mix was based on internet use by eight specific industry verticals: Enterprise, Small-to-Medium Businesses (SMB), Remote Office Branch Office (ROBO), Healthcare and Educational organizations, Media and Entertainment, and Financial and Retail organizations. As outlined in v1.6 of the SecureIQLab Advanced Cloud Firewall CyberRisk Validation Methodology, the primary objective of the security resiliency-based test is NOT to push the cloud security solution under test to its maximum limits but to ensure it remains operationally and functionally viable up to at least at 50% of its throughput.

The ability of the Amazon AWS Network Firewall to pass each stage of the security resiliency test was based on the following criteria:

- **PASS** = Security resiliency protection rate (%) must be ≥ 95% against all attacks under load.
- **PASS** = Overall solution throughput (%) must be ≥ 95% (at steady state) of the maximum tested ACFW cloud throughput numbers.

- **PASS** = Overall application traffic success rate (%) must be ≥ 95% of all real-world application traffic validated against a specific cloud-based scenario.

The Amazon AWS Network Firewall was tested for security resiliency under real-world scenarios during the entire test cycle, and Table 8 below provides the results from these tests.

Real World Cloud-based Traffic Scenario Mix	Security Resiliency Protection Rating	Overall Solution Throughput	Overall Application Traffic Success Rate
Media and Entertainment Companies	Contact SecureIQLab		
Healthcare Organization			
Financial Institution			
Enterprise			
Small-to-Medium Business (SMB)			
Educational Institution			
Retail Companies			
Remote office Branch Office (ROBO)			

Table 8. Security Resiliency

Contact SecureIQLab regarding AWS Network Firewall's Security Resiliency tests.

6. Operational Efficiency Results

ACFW operational efficiency measures the tested ACFW's operating burden and complexity of setup and use. As such, the Operational Efficiency Score measures both the ability of the ACFW to detect and respond to cyber-attacks appropriately and ease of use. The operational efficiency was evaluated by considering factors such as:

- The ease of tuning the ACFW security policy and configuration (pre-and-post deployment).
- The solution's incident response and management intuitiveness from a policy and security configuration perspective.
- Compliance check.
- Risk assessment and mitigation capabilities.
- Enhanced security metrics reporting capabilities.
- The ease of managing and controlling assets and business continuity with appropriate configuration and policy backup (with restoration).

In the analysis, the Amazon AWS Network Firewall was rated high, medium, or low across 12 operational efficiency categories, as identified in Table 8 below. For more details on each of the categories, please contact SecureIQLab.

The Amazon AWS Network Firewall was tested for operational efficiency, considering real-world enterprise procurement, deployment, and active scenarios throughout the test life cycle. Table 9 below presents an overall operational efficiency score of 65.6%.

Operational Efficiency	Amazon ACFW Score	SecureIQLab ACFW Group Test Average Score
Overall Operational Efficiency Score	65.6%	75.2%

Table 9. Overall Operational Efficiency Score

Amazon AWS Network Firewall solution had high operational efficiency capabilities in six of the 12 validated categories of operational efficiency, as highlighted in Table 10 below.

ACFW Operational Efficiency Metrics	Amazon AWS Network Firewall	SecureIQLab ACFW Group Test Average Score
Security Policy Configuration	High	Med
Security Policy Management	Med	High
Asset Management	High	High
Access Control	High	High
Compliance Management	Med	High
Business Continuity Management	Low	Med
Risk Assessment & Mitigation	Low	Med
Security Metrics Reporting	High	High
Backup & Restore	Low	Med
Analytics	High	Med
Customer Support	Low	Med
License Management	High	High

Table 10: Operational Efficiency Results.

Table 10 shows that the Amazon ACFW performed better than average in two of the 12 operational efficiency categories validated.

7. Key ACFW Solution Differentiators – Vendor Perspective

Amazon offers the following benefits for choosing the AWS Network Firewall:

AWS is a fully managed service that makes it easy to deploy essential network protections for all Amazon virtual private clouds. Including features that can prevent threats and provide protection against malicious network activity. Key features include:

Deploy with only a few clicks. It's easy to get started with AWS Network Firewall by visiting the Amazon VPC console to create or import your firewall rules group them into policies and apply them to the VPCs you want to protect AWS Network Firewall pricing is based on the number of firewalls deployed and the amount of traffic inspected there are no upfront commitments, and only pay only for what is used.

Automatically scales with network traffic. No need to worry about building and maintaining network security infrastructure.

Protect Workloads. Protect unique workloads with a flexible engine that can define thousands of custom rules. Users can define firewall rules that provide fine-grained control over network traffic. Additionally, the AWS Network Firewall supports the ability to subscribe to managed lists for IP, domain names, and threat signature. This feature allows users to define firewall rules to protect your unique workloads reducing the operational complexity of writing and updating rules to keep up with the constantly changing threat landscape rules can be based on IP port protocol domain and pattern matching and are written in common open-source rule formats.

Centrally manage security policies across multiple existing accounts and virtual private clouds (VPCs) through the AWS firewall manager. AWS Network Firewall works with AWS Firewall Manager to ensure mandatory security policies are automatically enforced on newly created accounts and VPCs.

Real-time activity monitoring through Amazon CloudWatch metrics. The CloudWatch home page automatically displays metrics about every AWS service in use. Create custom dashboards to display metrics for custom applications and display custom collections of metrics. Create alarms that watch metrics and send notifications or automatically make changes to the resources for when a threshold is breached. This data may be used to stop under-used instances to save money.

8. Conclusion

The Amazon AWS Network Firewall can enforce policy configuration and has inspection capabilities against some cloud relevant attacks. The AWS Network Firewall performed better than average for operational efficiency in the Security Policy Configuration and Analytics categories. The AWS Network Firewall earned perfect scores in three of the four Browser-Based threat categories. Also notable was Amazon's performance in the Network-based Advanced Evasive Techniques and Cloud-Centric Post Exploitation Techniques, where they blocked 100.0% of the attacks. AWS Network Firewall also boasts a significantly better than average False Positive Resistance score.

9. Contact Information

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

+1.512.575.3457

www.secureiqlab.com

info@secureiqlab.com

10. Copyright and Disclaimer

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

SecureIQLab (March 2024)