SecureIQlab®

REPORT

SecureIQLab Advanced Cloud Firewall (ACFW) v1.6 CyberRisk Comparative Report

Published: 21 March 2024

Report Contents

1. Introduction

With the evolution of the attack vectors and the dissolution of the traditional perimeter-based defenses, attacks on applications are the leading cause of breaches. Both client-centric and web application-based vulnerabilities are among the top breach vectors[1].

SecureIQLab conducted testing for 12[2] leading enterprise-class ACFW solutions. This test was conducted in accordance with the Anti-Malware Testing Standards Organization[3] (AMTSO) test standard. These results map to version v1.6 of the SecureIQLab Advanced Cloud Firewall CyberRisk Validation Methodology, AMTSO Test ID: AMTSO-LS1-TP070. This evaluation is the most comprehensive of its kind ever performed.

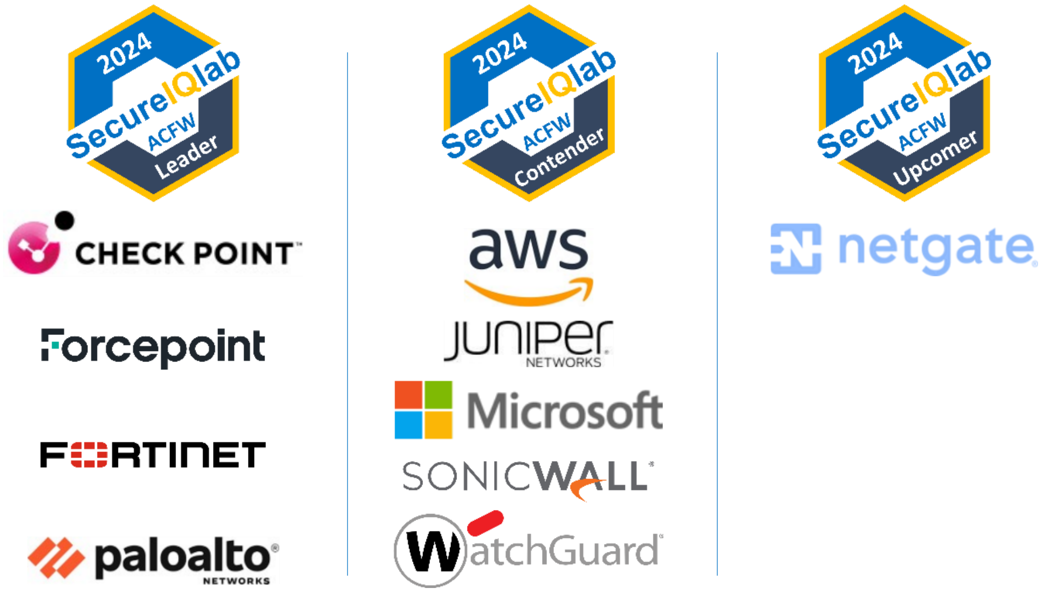

Figure 1. SecureIQLab Advanced Cloud Firewall v1.6 (ACFW) Security Vendors

This comparative report provides an overview of the results for all tested vendors. Vendors that completed testing are grouped alphabetically within ranking in Figure 1. The three rankings vendors fell into are Leader, Contender, and Upcomer. These rankings are derived from the CyberRisk Ripple in Figure 2 in the next section.

Test results have necessarily been simplified and presented for review in a summary format. In writing this report, SecureIQLab has made extensive efforts to guarantee the accuracy of the results while straightforwardly presenting them. There are also individual reports for each vendor, which are available at https://secureiqlab.com/publications/.

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

[2] Testing was attempted on a total of 12 Advanced Cloud Firewall solutions. Please click here for details.

[3] standards https://www.amtso.org/ conducted testing.

©SecureIQLab LLC, 2019 – 2024. All rights reserved.

2. SecureIQLab Advanced Cloud Firewall CyberRisk Ripple

The 2024 Advanced Cloud Firewall v1.6 (ACFW) CyberRisk Ripple[4] highlighted below in Figure 2 captures the security efficacy (represented in the Y-Axis) versus operational efficiency (represented in the X-axis) metrics of the different enterprise-class cloud firewall solutions validated against SecureIQLab ACFW v1.6 Methodology[5].

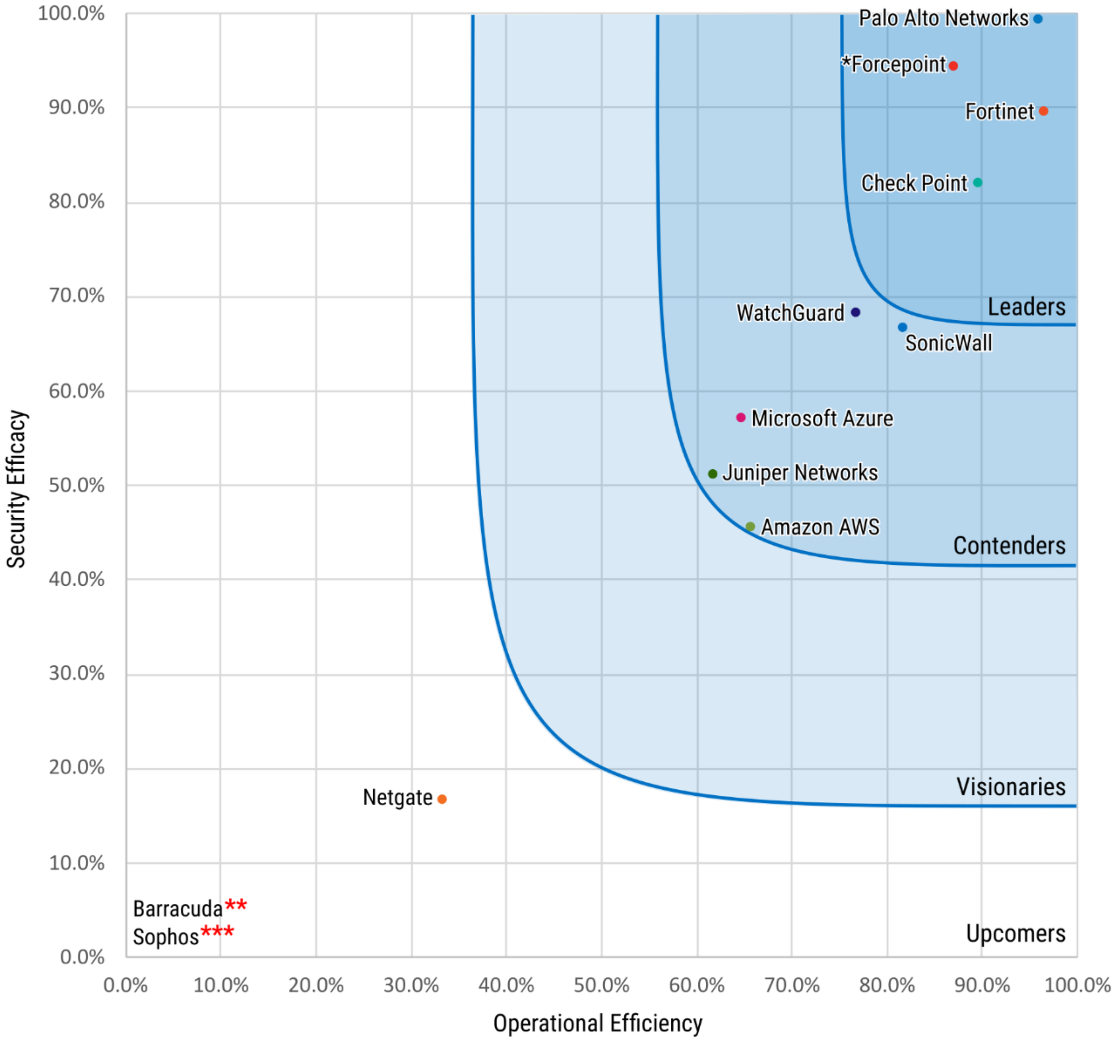

Figure 2. SecureIQLab 2024 Advanced Cloud Firewall v1.6 (ACFW) CyberRisk Ripple

[4] Please click here for details on the SecureIQLab ACFW CyberRisk Ripple.
[5] SecureIQLab ACFW v1.6 Methodology.
* Forcepoint results are the combined protection from their ACFW and Endpoint security solutions.
** Contact SecureIQLab for details.
*** Contact SecureIQLab for details.

©SecureIQLab LLC, 2019 – 2024. All rights reserved.

Vendor Name	Advanced Cloud Firewall Solution Details	Overall Security Efficacy Score (%)	Overall Operational Efficiency Score (%)	CyberRisk Ripple Category
Amazon AWS	AWS Network Firewall	45.8%	65.6%	Contender
Barracuda	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
Check Point	CloudGuard Network Security with Threat Prevention & SandBlast	82.1%	89.6%	Leader
Forcepoint	Forcepoint Next Generation Firewall & Endpoint Context Agent	94.4%	86.9%	Leader
Fortinet	FortiGate Next-Generation Firewall	89.6%	96.5%	Leader
Juniper Networks	vSRX Premium Next Generation Virtual Firewall with Anti-Virus Protection	51.3%	61.6%	Contender
Microsoft Azure	Azure Firewall (Premium)	57.3%	64.7%	Contender
Netgate (pfSense)	Netgate Pfsense Plus Firewall/VPN/Router	16.8%	33.3%	Upcomers
Palo Alto Networks	VM-Series Virtual NextGen Firewall w/ Adv. Security Subs	99.4%	95.8%	Leader
SonicWall	SonicWall NSv (Firewall/Security/VPN/Router)	66.8%	81.5%	Contender
Sophos	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
WatchGuard	WatchGuard Firebox Cloud	68.3%	76.7%	Contender

Table 1. SecureIQLab ACFW v1.6 Result Summary

Table 1 displays the test results of the vendors in alphabetical order; it shows the validation percentages and vendors' placement ranking within the ACFW CyberRisk ripple. Please click here more information on the SecureIQLab ACFW CyberRisk Ripple.

3. Security Efficacy Comparative Overview

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 from more than 1000 real-world 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 cloud firewall security solutions were tested against four primary security categories that are integral to validating the overall security efficacy: Common (standard) threats, advanced threats, SSL/TLS threat efficacy, and resistance to false positives (Operational Accuracy). Figure 3 below highlights the overall security efficacy scores of all tested cloud firewall solution vendors.

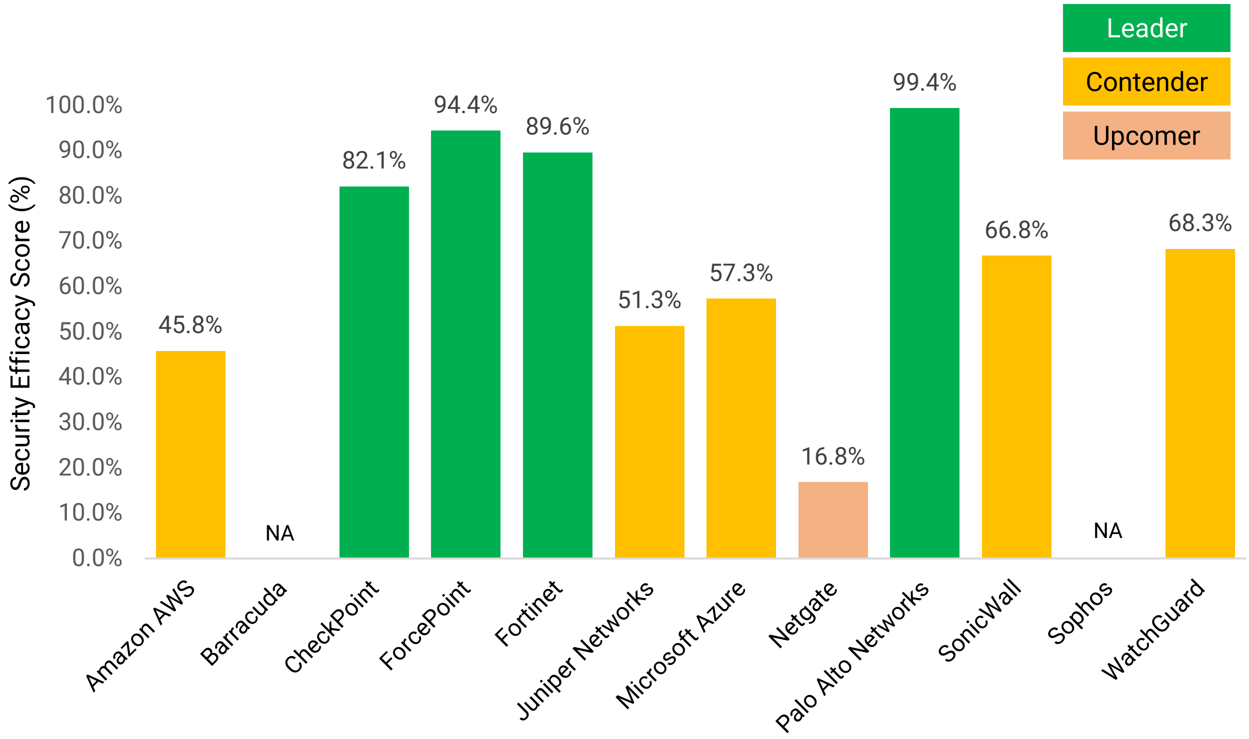

Figure 3. Overall Security Efficacy Score

©SecureIQLab LLC, 2019 – 2024. All rights reserved.

3.1 Common Cloud Firewall Threat Categories (Standard Threats)

The cloud firewall security solutions were tested against 13 attack types within four standard (common) threat categories: application-based threats, malware & botnets, browser-based threats, and data-loss & leakage.

Figure 4 below presents the Common (Standard) Cloud Firewall Threat average scores of the 12 Advanced Cloud Firewall solutions by averaging the scores for each threat type together within their respective attack category.

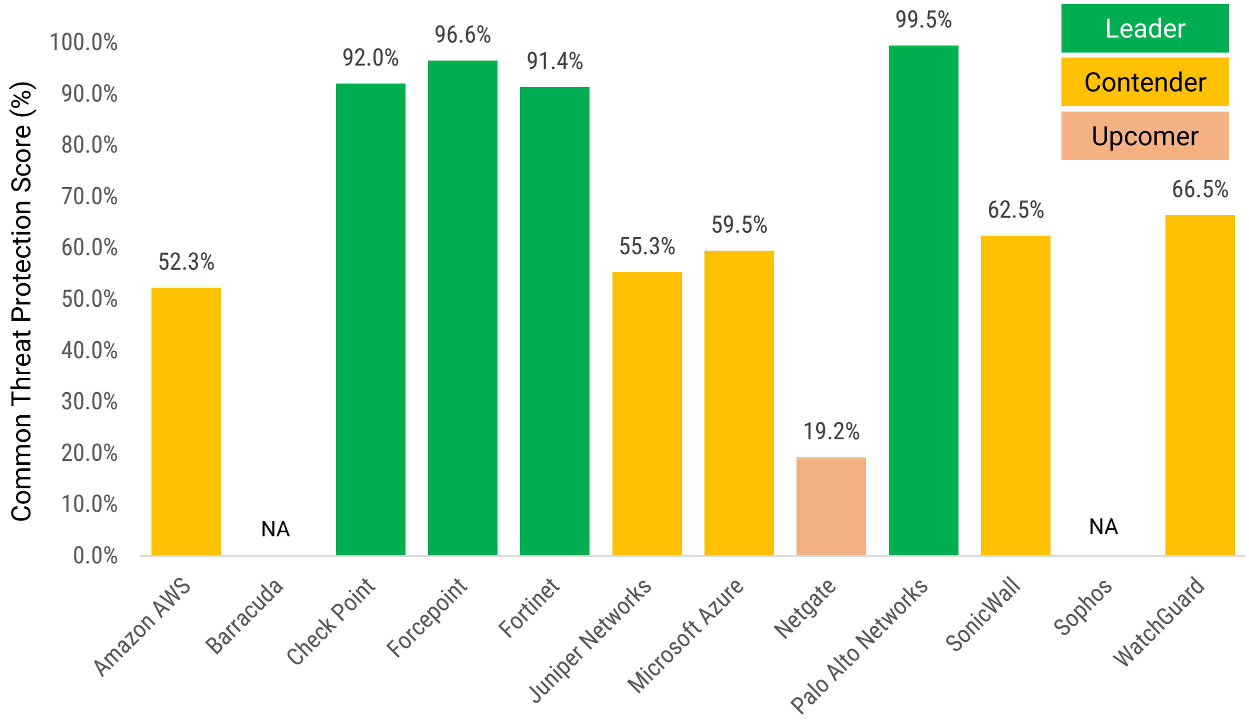

Figure 4. Common (Standard) Threat Protection Score

The top four vendors in this test were Check Point, Forcepoint, Fortinet, and Palo Alto Networks. Of these, Palo Alto Networks had the highest score.

3.2 Advanced Cloud Firewall Threat Categories

Advanced Cloud firewalls must extend their protective capabilities to counter advanced threats. Such threats may circumvent traditional security measures. 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 Advanced Threat Category Score consists of eight attack types classified as advanced threats which the security solutions were tested against. Figure 5 below provides the results from these tests.

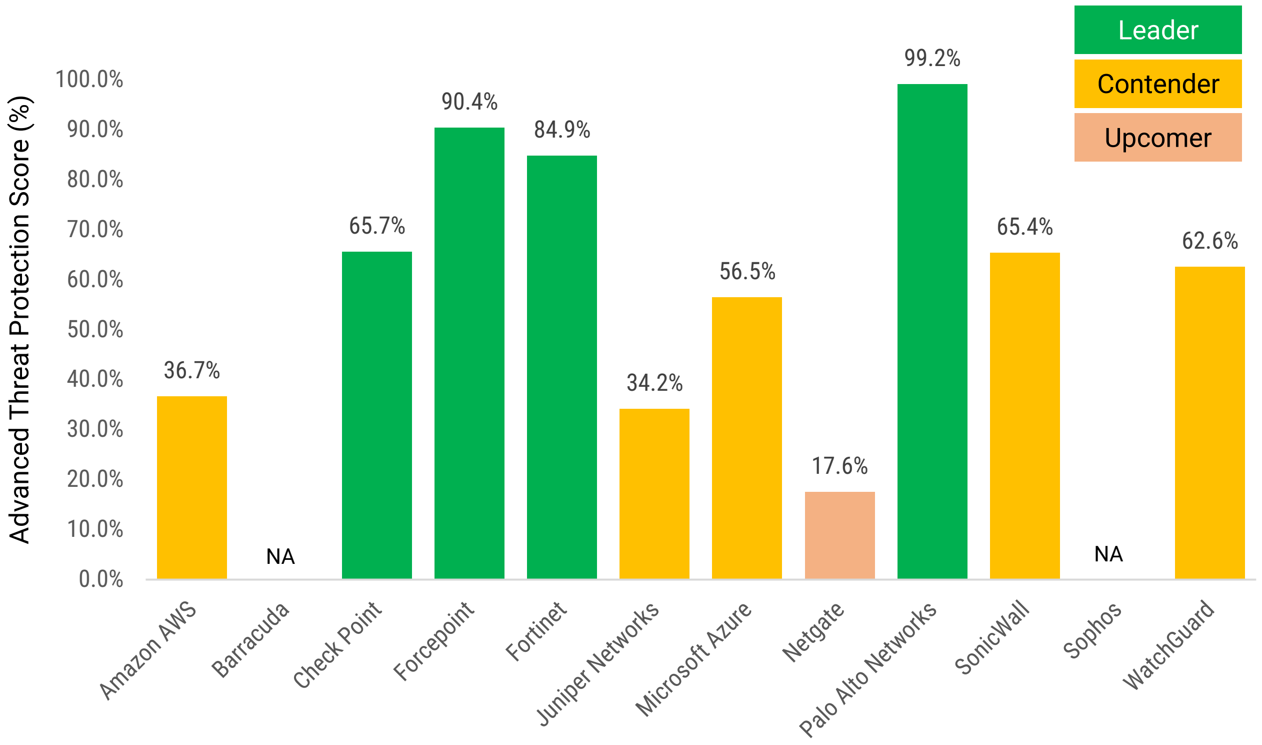

Figure 5. Advanced (Non-Standard) Threat Protection Score

The Advanced Cloud Firewall Threat average scores are calculated by averaging the scores for each threat type together within their respective attack category. The top four vendors in this test were Check Point, Forcepoint, Fortinet, and Palo Alto Networks. Of these, Palo Alto Networks scored the highest.

3.3 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 inhibits 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. Operational accuracy was performed using real-world scenarios during the entire test cycle, ensuring that the firewall products prevented malicious traffic without blocking normal enterprise operations and traffic conditions.

Table 2 below provides the results from these tests validated against the 12 cloud firewall solution vendors.

Vendor Name	Advanced Cloud Firewall Solution Details	Overall False Positive Score (%)
Amazon AWS	AWS Network Firewall	1.3%
Barracuda	Contact SecureIQLab	Contact SecureIQLab
Check Point	CloudGuard Network Security with Threat Prevention & SandBlast	0.0%
Forcepoint	Forcepoint Next Generation Firewall & Endpoint Context Agent	0.4%
Fortinet	FortiGate Next-Generation Firewall	0.4%
Juniper Networks	vSRX Premium Next Generation Virtual Firewall with Anti-Virus Protection	0.4%
Microsoft Azure	Azure Firewall (Premium)	1.3%
Netgate (pfSense)	Netgate Pfsense Plus Firewall/VPN/Router	Contact SecureIQLab
Palo Alto Networks	VM-Series Virtual NextGen Firewall w/ Adv. Security Subs	0.0%
SonicWall	SonicWall NSv (Firewall/Security/VPN/Router)	0.0%
Sophos	Contact SecureIQLab	Contact SecureIQLab
WatchGuard	WatchGuard Firebox Cloud	0.0%

Table 2. Operational Accuracy (False Positive) Detection Score

The overall false positive detection was exceptional for seven of the 12 vendors who had a false positive score of < 0.5%, achieving a near-perfect score. Check Point, Palo Alto Networks, and WatchGuard had perfect False Positive Scores.

3.4 ACFW SSL/TLS Support

SecureIQLab tested 22 of the TLS v1.2 ciphers and 3 TLS v1.3 ciphers against each of the ACFWs. 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 cloud firewall solutions were tested for overall SSL/TLS threat efficacy and its ability to protect against attacks delivered through the supported ciphers in real-world scenarios. Table 3 below presents the results of these ACFW solutions successfully identified, detected, and prevented all the attacks throughout the entire SSL/TLS test cycle on all supported ciphers.

©SecureIQLab LLC, 2019 – 2024. All rights reserved.

Vendor Name	Overall SSL/TLS Cipher Security Efficacy Score (%)	Total No. of TLS v1.2 Ciphers Supported	Total No. of TLS v1.3 Ciphers Supported
Amazon AWS	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
Barracuda	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
Check Point	95.6%	18/22	3/3
Forcepoint	100.0%	22/22	3/3
Fortinet	100.0%	22/22	3/3
Juniper Networks	100.0%	22/22	3/3
Microsoft Azure	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
Netgate (pfSense)	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
Palo Alto Networks	100.0%	19/22	3/3
SonicWall	88.0%	19/22	3/3
Sophos	Contact SecureIQLab	Contact SecureIQLab	Contact SecureIQLab
WatchGuard	100.0%	22/22	3/3

Table 3. SSL/TLS Cipher Security Efficacy

The cipher suites for TLS v1.2 and TLS v1.3 as highlighted in Table 3 above, were tested against all the cloud firewall solutions with more than half of them having exceptional coverage and having the ability to successfully handle packet decryption and inspection[6].

4. 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).

[6] Please refer to the individual test reports for supported cyphers https://secureiqlab.com/publications/

©SecureIQLab LLC, 2019 – 2024. All rights reserved.

In this analysis, the cloud firewall solution security vendors were rated high, medium, or low across 12 operational efficiency categories, as identified in Table 5 below. For more details on each of the categories, please contact SecureIQLab.

Operational Efficiency Metrics	Amazon AWS	Barracuda	Check Point	Forcepoint	Fortinet	Juniper	Microsoft Azure	Netgate (pfSense)	Palo Alto Networks	SonicWall	Sophos	WatchGuard
Security Policy Configuration	High	Contact SecureIQLab	High	High	High	Med	Med	Low	High	Med	Contact SecureIQLab	High
Security Policy Management	Med		High	High	High	Med	Med	Med	High	High		Med
Asset Management	High		Med	High	High	Low	High	Low	High	High		High
Access Control	High		High	High	High	High	High	Low	High	High		Med
Compliance Management	Med		High	High	High	High	Med	Low	High	High		High
Business Continuity Management	Low		High	High	High	High	Low	Low	High	Low		High
Risk Assessment & Mitigation	Low		High	Low	High	Low	High	Low	High	High		High
Security Metrics Reporting	High		High	High	High	High	High	Low	High	High		High
Backup & restore	Low		High	High	High	High	Low	Low	High	High		Med
Analytics	High		High	High	High	Med	Med	Low	High	High		Med
Customer Support	Low		High	High	High	High	Low	Low	High	High		High
License Management	High		High	Low	High	High	High	Med	High	High		High

Table 4. Operational Efficiency Results

©SecureIQLab LLC, 2019 – 2024. All rights reserved.

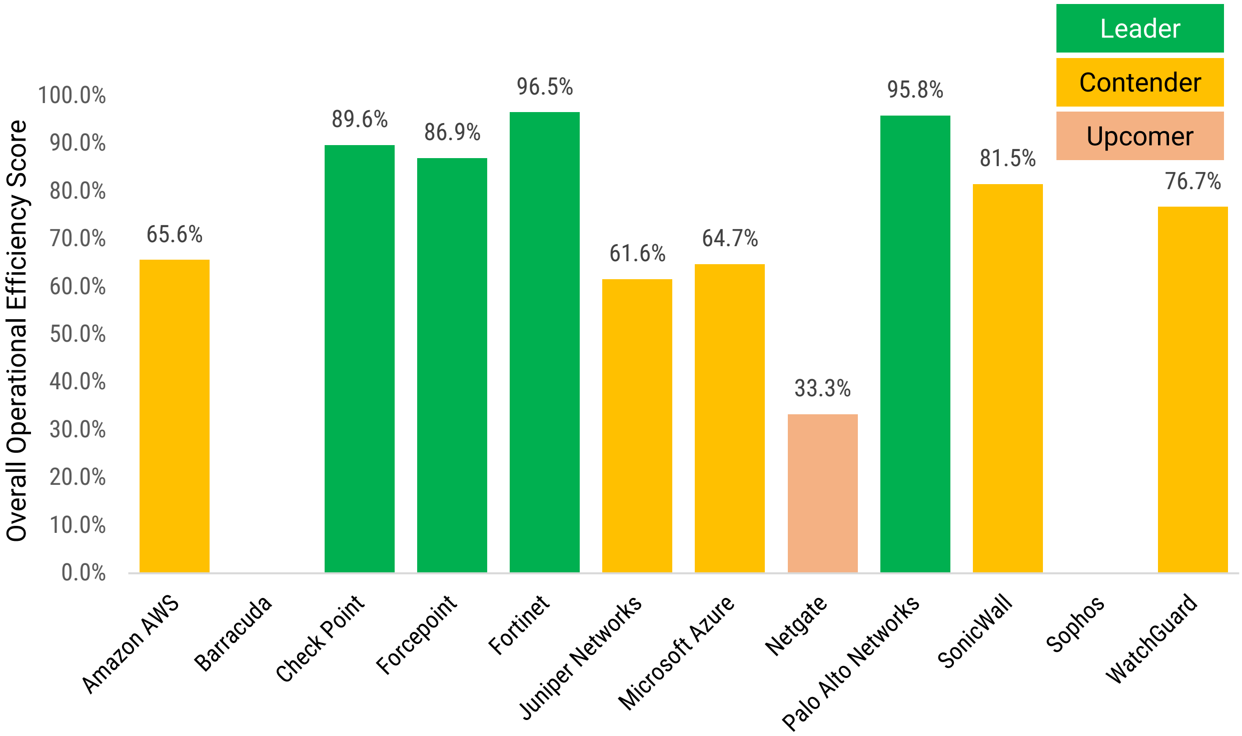

Figure 6. Overall Operational Efficiency Score

The top four vendors in this test were Check Point, Forcepoint, Fortinet, and Palo Alto Networks. Of these, Fortinet scored the highest of the 12 validated categories of operational efficiency.

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 founded on real-world scenarios. The traffic mix was based on internet use by eight specific industry verticals: Media and Entertainment, Healthcare Organization, Financial Institution, Enterprise, Small-to-Medium Businesses (SMB), Education Institution, Retail companies, and Remote Office Branch Office (ROBO). 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 Advanced Cloud Firewall solutions were tested for security resiliency under real-world scenarios during the entire test cycle, and Table 4 below provides the results from these tests, wherein only seven vendors passed the SecureIQLab security resiliency standard against overall throughput, application failure rate and security efficacy.

Real-world Traffic Scenarios	Amazon AWS	Barracuda	Check Point	Forcepoint	Fortinet	Juniper	Microsoft Azure	Netgate (pfSense)	Palo Alto Networks	SonicWall	Sophos	WatchGuard
Media and Entertainment	Contact SecureIQLab	Contact SecureIQLab	↗	↗	↗	↗	Contact SecureIQLab	Contact SecureIQLab	↗	↗	Contact SecureIQLab	↗
Healthcare Organization			↗	↗	↗	↗			↗	↗		↗
Financial Institution			↗	↗	↗	↗			↗	↗		↗
Enterprise			↗	↗	↗	↗			↗	↗		↗
Small-to-Medium Business (SMB)			↗	↗	↗	↗			↗	↗		↗
Educational Institution			↗	↗	↗	↗			↗	↗		↗
Retail Companies			↗	↗	↗	↗			↗	↗		↗
Remote office Branch Office (ROBO)			↗	↗	↗	↗			↗	↗		↗

Table 4. Security Resiliency

↗ Resiliency Icon: Passed SecureIQLab Security Resiliency Rating Standard

6. Conclusion

SecureIQLab has released the first-of-its-kind comprehensive ACFW report that evaluates:

- 12 key areas of operational efficiency.
- Security resiliency as a concept to withstand and absorb security attacks.
- Security efficacy in terms of cyber threat actors and cyber threat techniques as it relates to key operational domain as cloud.

SecureIQLab will further abstract the concept of “secure by design” and “secure by default” in key technology domains, such as the cloud as it applies to ACFW, in the next iteration of our ACFW test methodology.

7. Contact Information

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

+1.512.575.3457

www.secureiqlab.com

info@secureiqlab.com

8. Copyright and Disclaimer

Copyright © 2024 SecureIQLab, LLC. All rights reserved. The content of this report is protected by United States and international copyright laws and treaties. You may only use this report for your personal, non-commercial, informational purposes. Without SecureIQLab's prior written consent, you may not: (i) reproduce, modify, adapt, create derivative works from, publicly perform, publicly display, or distribute this report; or (ii) use this report, the SecureIQLab name, or any SecureIQLab trademark or logo as part of any marketing, promotion, or sales activities. THIS REPORT IS PROVIDED "AS IS," "AS AVAILABLE" AND "WITH ALL FAULTS." TO THE MAXIMUM EXTENT PERMITTED BY LAW, SECUREIQLAB EXPRESSLY DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING: (a) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; AND (b) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF THE REPORT, OR THAT USE OF THE REPORT WILL BE ERROR-FREE, UNINTERRUPTED, FREE FROM OTHER FAILURES OR WILL MEET YOUR REQUIREMENTS. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING SENTENCE, YOU ACKNOWLEDGE AND AGREE THAT THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT DEPEND UPON VARIOUS FACTORS, INCLUDING FACTORS OUTSIDE OF SECUREIQLAB'S CONTROL, SUCH AS: (1) THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF INFORMATION AND MATERIALS PROVIDED BY OTHER PARTIES THAT ARE RELIED UPON BY SECUREIQLAB IN PERFORMING PREPARING THE REPORT; AND (2) THE UNDERLYING ASSUMPTIONS MADE BY SECUREIQLAB IN PREPARING THE REPORT REMAINING TRUE AND ACCURATE. YOU ARE SOLELY RESPONSIBLE FOR INDEPENDENTLY ASSESSING THE QUALITY, ACCURACY, CURRENCY AND COMPLETENESS OF THE REPORT BEFORE TAKING OR OMITTING ANY ACTION BASED UPON THE REPORT. IN NO EVENT WILL SECUREIQLAB BE LIABLE FOR ANY LOST PROFITS OR COST OF COVER, OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE OR CONSEQUENTIAL DAMAGES, INCLUDING DAMAGES ARISING FROM OR RELATING TO ANY TYPE OR MANNER OF COMMERCIAL, BUSINESS OR FINANCIAL LOSS, EVEN IF SECUREIQLAB HAD ACTUAL OR CONSTRUCTIVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE.

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

SecureIQLab (March 2024)