



# SecureIQlab<sup>®</sup>

## REPORT

### CyberRisk Validation Report – Forcepoint

Product Version: Forcepoint Next Generation Firewall (NGFW) v7.1

Published: 21 March 2024

Report Contents

1. Introduction..... 2

2. Report Summary..... 3

3. ACFW Test Overview ..... 4

    3.1 ACFW Deployment Overview ..... 4

4. Security Efficacy Results..... 5

    4.1 Common Cloud Firewall Threat Categories (Standard Threats)..... 5

    4.2 Advanced Cloud Firewall Threat Categories ..... 7

    4.3 Operational Accuracy Category..... 7

    4.4 ACFW SSL/TLS Support ..... 8

5. Security Resiliency Results ..... 10

6. Operational Efficiency Results..... 11

7. Key ACFW Solution Differentiators – Vendor Perspective ..... 13

8. Conclusion ..... 14

9. Contact Information ..... 14

10. Copyright and Disclaimer..... 14

## 1. Introduction

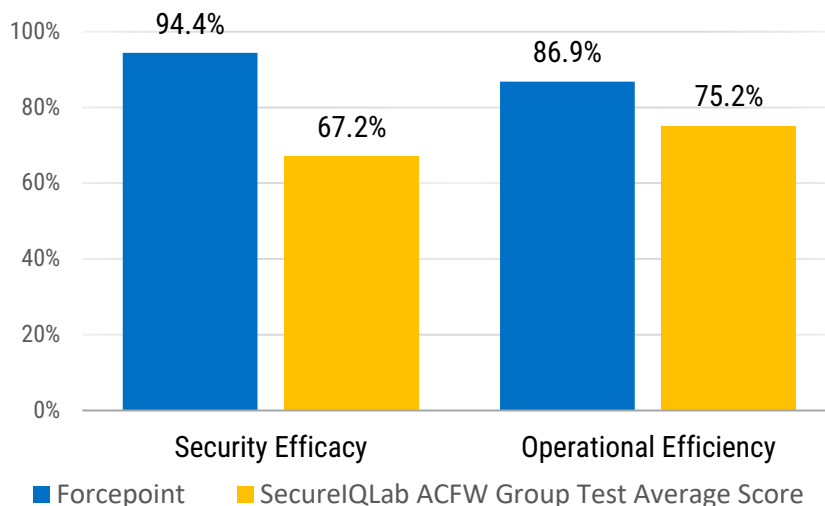


Figure 1. Summary results for Forcepoint vs the ACFW Group Test Scores

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.

SecureQLab conducted testing for 12<sup>1</sup> leading enterprise-class ACFW solutions. This test was conducted in accordance with the Anti-Malware Testing Standards Organization<sup>2</sup> (AMTSO) test Standard. The maps to version v1.6 of the SecureQLab 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, SecureQLab completed testing Forcepoint Next Generation Firewall (NGFW). This report discusses the test results for the Forcepoint Next Generation Firewall (NGFW) v7.1, and includes validation of the following security modules and components: Anti-Malware, Client Protection, ECA Settings, Global Threat Intelligence, URL Filtering, Sandbox, Server Protection, and Threat Seeker,

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

As Figure 1 shows visually, Forcepoint Next Generation Firewall (NGFW) was superior to the average ACFW tested.

In writing this report, SecureQLab 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.

<sup>1</sup> Testing was attempted on a total of 12 Advanced Cloud Firewall solutions. Please [click here](#) for details.

<sup>2</sup> Standards <https://www.amtso.org/conducted-testing>.

2. Report Summary

This 2024 Advanced Cloud Firewall CyberRisk Validation Report provides test results for the Forcepoint Next Generation Firewall (NGFW). 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 Forcepoint Next Generation Firewall (NGFW) solution validated against SecureQLab ACFW v1.6 methodology.

ACFW Test Categories	Forcepoint ACFW Score	SecureQLab ACFW Group Test Average Score
Security Efficacy	94.4%	67.2%
Resistance to False Positives	99.6%	89.8%
Operational Efficiency	86.9%	75.2%
SSL/TLS Security Efficacy	100%	68.4%

Table 1. Forcepoint ACFW Result Summary

Figure 2 presents the above table in visual format.

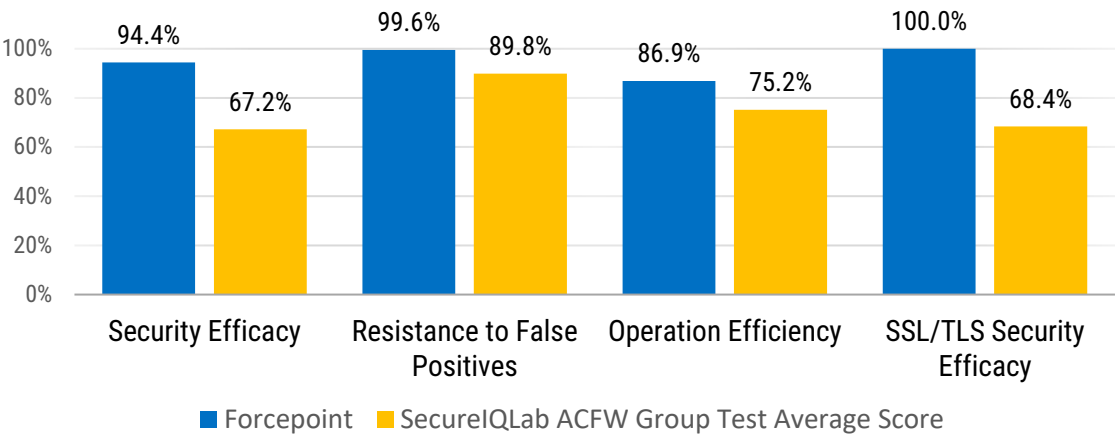


Figure 2. Overall Result Summary: Forcepoint ACFW vs SecureQLab ACFW Group Test Average

Overall Result Summary: Forcepoint Next Generation Firewall (NGFW) did exceptionally well compared to the overall SecureQLab ACFW group test average in all the primary enterprise categories as represented in the SecureQLab ACFW validation methodology selection criteria.<sup>3</sup>

<sup>3</sup> [SecureQLab 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.

SecureQLab 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 SecureQLab 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”. SecureQLab then performed any required tuning according to recommended vendor best practices for operational scenarios involving cloud deployments<sup>4</sup>.

#### 3.1 ACFW Deployment Overview

Per SecureQLab'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, SecureQLab 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 SecureQLab 2023 [ACFW CyberRisk Validation Methodology](#) (AMTSO Test ID: AMTSO-LS1-TP070).

<sup>4</sup> [Forcepoint 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 SecureQLab reflects our commitment to innovation and continuous improvement. Moving forward, SecureQLab plans to continue to augment attack libraries and incorporate additional relevant operational metrics as needed in future iterations of this test.

The Forcepoint Next Generation Firewall (NGFW) 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 SecureQLab findings during the security effectiveness validation and reporting of the Forcepoint Next Generation Firewall (NGFW). 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.

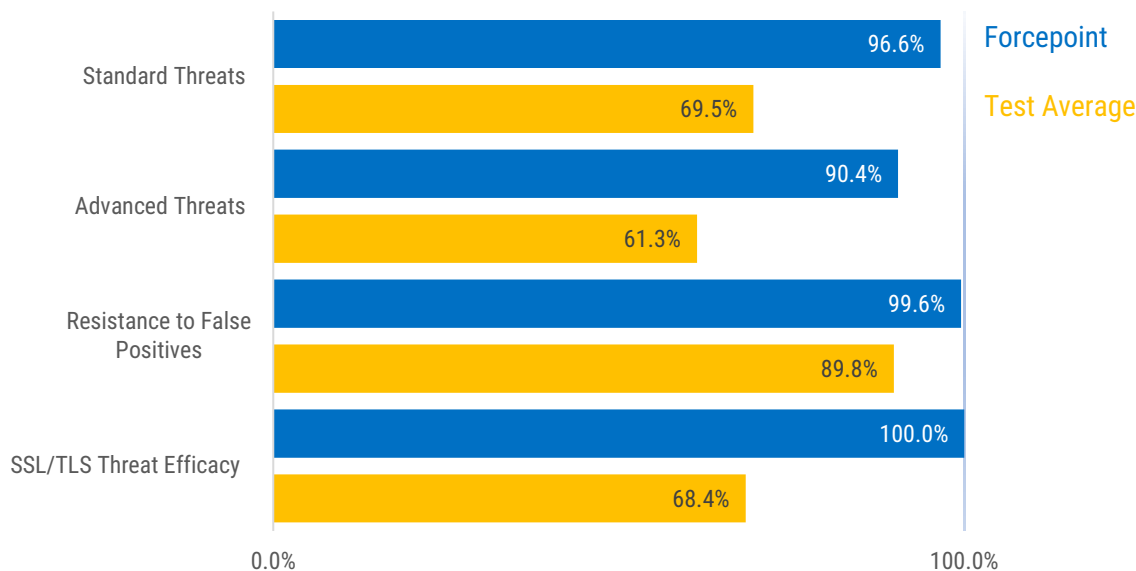


Figure 3. Forcepoint Advanced Cloud Firewall Security Effectiveness

### 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	Forcepoint ACFW Inspection Score	SecureQLab ACFW Group Test Average Score
<b>Application-Based Threats</b>		
Cross-Site Scripting (XSS) Attacks – HTTP	100.0%	75.5%
Cross-Site Scripting (XSS) Attacks – HTTPS	100.0%	67.1%
Malicious URL Attacks	100.0%	68.0%
<b>Malware &amp; Botnets</b>		
Malware Download over HTTPS	100.0%	61.3%
Compressed Malicious Files	90.8%	60.2%
Botnets	100.0%	58.3%
<b>Browser-Based Threats</b>		
Browser Exploits	100.0%	74.0%
Cookie Stealing - HTTP	75.0%	85.0%
Cookie Stealing - HTTPS	100.0%	100.0%
Browser Version and Plugin-in Control	100.0%	60.0%
Obfuscated JavaScript	100.0%	90.0%
<b>Data-loss and Leakage</b>		
Phishing Site-Based Attacks	95.7%	56.6%
Adware Site Prevention	PASS	PASS
<b>Standard Threats Average Score</b>	<b>96.6%</b>	<b>69.5%</b>

Table 2. Standard Threats Protection Testing

The Forcepoint NGFW demonstrates superior blocking capabilities compared to the average and scored 100% in all but three 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 Forcepoint Next Generation Firewall (NGFW) was tested against eight attack types classified as advanced threats. Table 3 below provides the results from these tests.

Advanced Threat Classification	Forcepoint ACFW Inspection Score	SecureQLab ACFW Group Test Average Score
Advanced Evasive Techniques (Application-based)	100.0%	79.6%
Advanced Evasive Techniques (Network-based)	100.0%	75.0%
Known Malicious Files	100.0%	60.2%
Malicious Documents	100.0%	59.3%
Active Cloud-Based Threats (aka Active Threats)	23.5%	46.5%
Advanced Persistent Threats (APT)	100.0%	65.0%
Cloud-Centric Post Exploitation Techniques (Post-Exploitation – DNS Tunnelling)	100.0%	45.0%
Cloud-Centric Post Exploitation Techniques (Post-Exploitation – ICMP Tunnelling)	100.0%	60.0%
<b>Advanced Threats Average Score</b>	<b>90.4%</b>	<b>61.3%</b>

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. Forcepoint performed well in these tests compared to the average and again scored 100% in all but one category.

## 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. SecureQLab 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 Forcepoint Next Generation Firewall (NGFW) 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	Forcepoint ACFW Score	SecureQLab ACFW Group Test Average Score
Resistance to False Positive Test	99.6%	89.8%

Table 4. Operational Accuracy

The Forcepoint Next Generation Firewall (NGFW) performed above average in this test and achieved a near perfect score.

#### 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, SecureQLab 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 Forcepoint Next Generation Firewall (NGFW) was tested for overall SSL/TLS threat efficacy and its ability to protect against attacks delivered through the supported ciphers in real-world scenarios. The Forcepoint ACFW successfully identified, detected, and prevented all the attacks throughout the entire SSL/TLS test cycle on tested ciphers. Table 5 below presents the results of these tests.

SSL/TLS Threat Efficacy Test	Forcepoint ACFW Overall Metric	SecureQLab ACFW Group Test Average Score
Overall SSL/TLS Security Efficacy	100.0%	68.4%

Table 5. SSL/TLS Threat Efficacy

The Forcepoint Advanced Cloud Firewall performed better than average and obtained a perfect score. This is notable given that the average was so low.

The cipher suites for TLS v1.2, as highlighted in Table 6 below, were tested for the Forcepoint Next Generation Firewall (NGFW).

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

Table 6. TLS v1.2 cipher Support

The Forcepoint Advanced Cloud Firewall passed all TLS v1.2 cyphers tested.

The cipher suites for TLS v1.3, as highlighted in Table 7 below, were tested for the Forcepoint Next Generation Firewall (NGFW).

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

Table 7. TLS v1.3 cipher Support

As can be seen from the above, the Forcepoint ACFW was able to successfully handle packet decryption and inspection.

## 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 Forcepoint Next Generation Firewall (NGFW) to pass each stage of the security resiliency test was based on the following criteria:

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

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

The Forcepoint Next Generation Firewall (NGFW) 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	Pass	Pass	Pass
Healthcare Organization	Pass	Pass	Pass
Financial Institution	Pass	Pass	Pass
Enterprise	Pass	Pass	Pass
Small-to-Medium Business (SMB)	Pass	Pass	Pass
Educational Institution	Pass	Pass	Pass
Retail Companies	Pass	Pass	Pass
Remote office Branch Office (ROBO)	Pass	Pass	Pass

Table 8. Security Resiliency

The Forcepoint Advanced Cloud Firewall passed all 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 Forcepoint Next Generation Firewall (NGFW) 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 SecureQLab](#).

The Forcepoint Next Generation Firewall (NGFW) was tested for operational efficiency, considering real-world enterprise procurement, deployment, and active scenarios throughout the test life cycle. Table 9 below presents an impressive overall operational efficiency score of 86.9%.

Operational Efficiency	Forcepoint ACFW Score	SecureQLab ACFW Group Test Average Score
Overall Operational Efficiency Score	86.9%	75.2%

Table 9. Overall Operational Efficiency Score

The Forcepoint Next Generation Firewall (NGFW) solution had high operational efficiency capabilities in 10 of the 12 validated categories of operational efficiency, as highlighted in Table 10 below.

ACFW Operational Efficiency Metrics	Forcepoint Next Generation Firewall (NGFW)	SecureQLab ACFW Group Test Average Score
Security Policy Configuration	High	Med
Security Policy Management	High	High
Asset Management	High	High
Access Control	High	High
Compliance Management	High	High
Business Continuity Management	High	Med
Risk Assessment & Mitigation	Low	Med
Security Metrics Reporting	High	High
Backup & Restore	High	Med
Analytics	High	Med
Customer Support	High	Med
License Management	Low	High

Table 10: Operational Efficiency Results.

Table 10 shows that the Forcepoint Advanced Cloud Firewall performed better than average.

## 7. Key ACFW Solution Differentiators – Vendor Perspective

Forcepoint states that their NGFW engines stand out in the market with three core aspects:

- Robust security efficacy
- Centralized management
- SD-WAN capabilities

At its core, multi-layer inspection combines access control, application identification, deep inspection, and file filtering for strong network security. Forcepoint's advanced traffic inspection provides real-time protection against threats like active exploits, malware, and botnets attacks. Administrators can quickly respond to threats with detailed packet inspection and correlation capabilities, blocking suspicious packets and terminating unwanted connectivity. These real-time actions, aligned with security policies, safeguard critical data and applications from harm. Integration with its included Endpoint Context Agent (ECA) enhances visibility into endpoint devices, providing granular details on users, device, and applications, delivering a deeper understanding of network access. When it comes to application types, ECA provides detailed information to the NGFW engines, enabling them to differentiate between sanctioned and unsanctioned applications. To safeguard networks against malware, NGFW engines can detect and block traffic. For instance, in the event of a malware attack using PowerShell, NGFW will block traffic originating from the PowerShell source. Forcepoint's ECA was instrumental in improving their security efficacy in the Advanced Cloud Firewall Threat Categories for Advanced Evasive Techniques and Advanced Persistent Threats.

The Secure SD-WAN Manager Console (SMC) serves as the central hub for unified configuration, monitoring, and reporting in the NGFW solution. It streamlines deployment across various locations, allowing administrators to handle both small and large deployments effortlessly from a single location. The SMC provides the flexibility to scale NGFW engines without sacrificing security or ease of use. Additionally, the SMC offers automated responses to security threats by instantly blocking unwanted traffic, reducing the need for immediate human intervention. The ability to import and export configurations between systems eliminates tedious configuring tasks, enhancing efficiency and accuracy in management.

Forcepoint NGFW offers native SD-WAN functionality, addressing traditional network infrastructure challenges. With features such as High Availability clustering and patented Multi-Link™ technology, organizations optimize bandwidth usage, ensure business continuity, and enhance network scalability and resilience. Multi-Link™ technology ensures network resilience through automated failover, providing seamless connectivity and comprehensive protection for branches. Moreover, the Application Health Monitoring (AHM) capability provides insights into application performance. Combined with SD-WAN optimization, it ensures optimal connectivity, resulting in enhanced efficiency. High Availability clustering eliminates single points of failure to ensure network resources are always available to users. This is crucial for maintaining productivity and preventing business disruptions.

## 8. Conclusion

The Forcepoint with Anti-Malware, Client Protection, File Reputation, Sandbox, Server Protection, and Threat Seeker modules performed impressively in our test. Forcepoint was above average in all categories tested. In threat detection and response, it was not only above average, but it was also above average by a significant margin. In threat detection and response, it was near the top score. Forcepoint did this while being above average at avoiding false positives, and while maintaining sufficient ease of use to have above-average operational efficiency.

## 9. Contact Information

SecureQLab, LLC.  
9600 Great Hills Trail Suite #150W  
Austin, TX 78759 USA  
  
+1.512.575.3457  
  
[www.secureiqlab.com](http://www.secureiqlab.com)  
[info@secureiqlab.com](mailto:info@secureiqlab.com)

## 10. Copyright and Disclaimer

Copyright © 2024 SecureQLab, 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 SecureQLab'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 SecureQLab name, or any SecureQLab 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, SECUREQLAB 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 SECUREQLAB'S CONTROL, SUCH AS: (1) THE QUALITY, ACCURACY, CURRENCY OR COMPLETENESS OF INFORMATION AND MATERIALS PROVIDED BY OTHER PARTIES THAT ARE RELIED UPON BY SECUREQLAB IN PERFORMING PREPARING THE REPORT; AND (2) THE UNDERLYING ASSUMPTIONS MADE BY SECUREQLAB 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 SECUREQLAB 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 SECUREQLAB HAD ACTUAL OR CONSTRUCTIVE KNOWLEDGE OF THE POSSIBILITY OF SUCH DAMAGES AND REGARDLESS OF WHETHER SUCH DAMAGES WERE FORESEEABLE.

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

SecureQLab (March 2024)