2024 AT&T Dynamic Defense CyberRisk Validation Report – Summary

Test Period: 15 July 2024 – 5 August 2024

Last Revision: 9 October 2024 | Commissioned by: AT&T

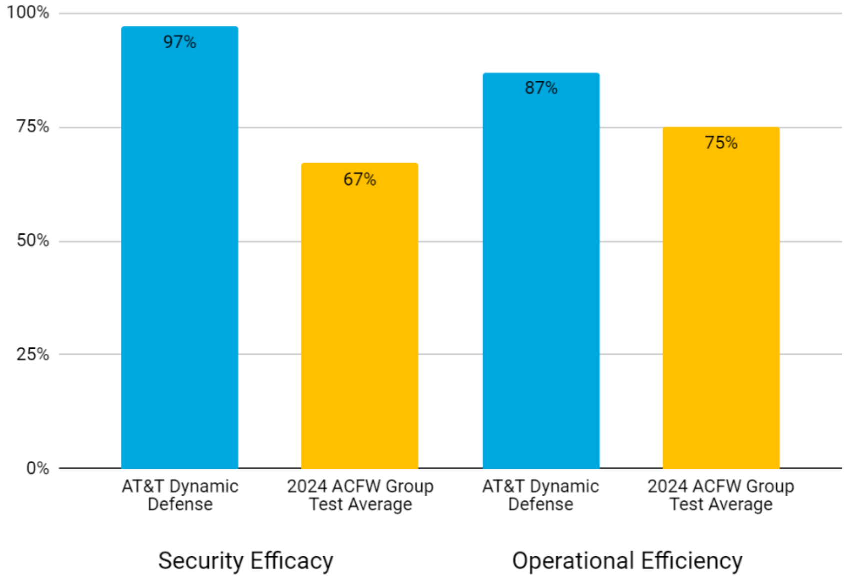

Figure 1. AT&T Dynamic Defense Security and Operational Summary Results

The 2024 SecureIQLab AT&T Dynamic Defense Cyber Risk Validation Report summary[1] provides test results on the Premium package for the AT&T Dynamic Defense solution. AT&T's Dynamic Defense test results for Security Efficacy and Operational Efficiency are shown in blue in Figure 1. The group average results from SecureIQLab's 2024 Public Advanced Cloud Firewall Testing are shown in orange for comparison. Our finding is that AT&T has significantly improved its firewall offering and its AI-based configuration assistance significantly improves ease of use.

AT&T Dynamic Defense is a comprehensive network security solution that provides dynamic IP blocking, stateful firewall monitoring, and Geo IP filtering. It leverages AI-based policy generation to simplify configuration and improve operational efficiency. SecureIQLab's 2024 evaluation shows exceptional performance in terms of security efficacy, especially in protecting networks from spyware, data exfiltration, and advanced persistent threats. This report highlights:

- Benefits of “Clean Pipes” AKA the prefiltering of traffic for malicious content.
- AT&T’s simplified onboarding through AI suggestion-based configuration.
- Dynamic Defense’s security efficacy and operational efficiency.
- Dynamic Defense’s operation accuracy, or resistance to false positives.

[1] Full report available here.

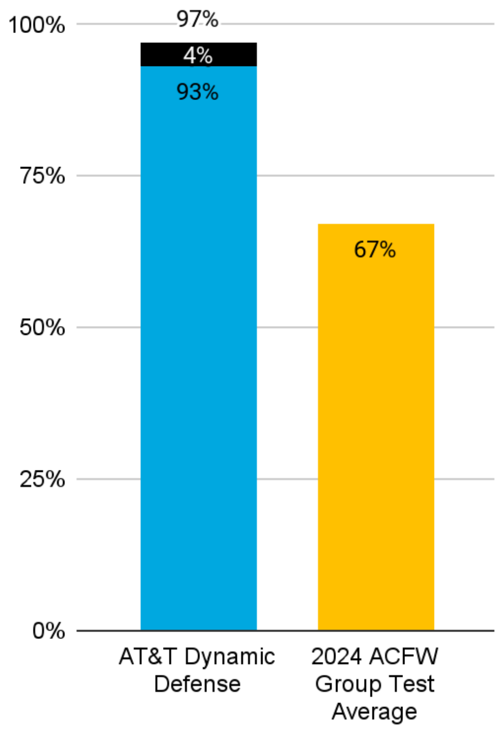

Figure 2. AT&T Dynamic Defense Security Score compared to the 2024 ACFW Group Average

Security Efficacy

The security efficacy test stressed measuring the effectiveness of AT&T Dynamic Defense's threat detection capabilities. As such, this test focused on AT&T Dynamic Defense's intrusion prevention system. The attacks launched included exploits targeting lift and shift applications, cloud-native application-centric exploits, post-exploitation activity, and advanced persistent threat (APT) activity. As seen in Figure 2, the overall security efficacy score of the AT&T Dynamic Defense was 97%, which is exceptional. Figure 2 shows that this 97% is composed of 93% traditional security measures, in blue, and 4% from AT&T Dynamic Defense Shield, in black. This highlights the contribution that AT&T Threat Intelligence provides as "Clean Pipes".

AT&T Dynamic Defense Shield

AT&T Dynamic Defense Shield, powered by AT&T's threat intelligence, automatically blocks traffic to and from malicious IP addresses within your network. It leverages a globally maintained blocklist that is continuously updated to reflect the latest threat landscape.

Testing was performed against a list of malicious IPs and simulated traffic outbound to these IP addresses. AT&T Dynamic Defense Shield blocked the traffic going to these destinations, demonstrating that the firewall has "PASSED" the test.

Premium Threat Protection / Protection+

The Premium Threat Protection package, previously known as Protection+, enhances AT&T Dynamic Defense's security features and adds Next-generation firewall capabilities to the product. It offers virus protection, spyware protection, and vulnerability protection. SecureIQLab ran various categories of tests that evaluate the capabilities of Premium Threat Protection.

AT&T Dynamic Defense was tested against 160 attack types within four threat categories. Figure 3 presents an overview of the SecureIQLab findings during the security effectiveness validation and reporting of the AT&T Dynamic Defense. This includes the application threats, post-exploitation, and APT activity score.

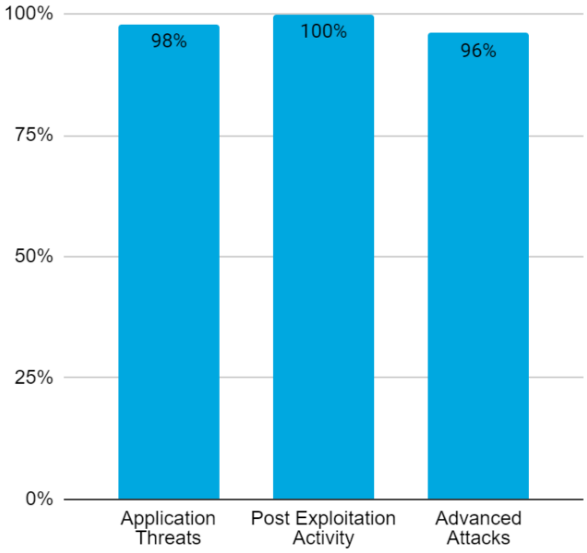

Figure 3. AT&T Dynamic Defense Security Efficacy Details

Policy Enforcement

AT&T Dynamic Defense demonstrated robust policy enforcement, successfully passing all tests related to application control, web/URL filtering, service control, IP control, and geo-filtering. As shown in Tabe 1, the solution was able to block or allow traffic based on configured rules, providing an effective and secure network environment.

Policy Enforcement Category	Results
Application Control	PASS
Web/URL Filtering	PASS
Service Control Policy	PASS
IP Control	PASS
Geo Filtering	PASS

Table 1. Policy Enforcement Categories and Results

Operational Accuracy Validation

Operational Accuracy Test	Results
Resistance to False Positives	100.0%

Table 2. Operational Accuracy

False positive testing was performed simultaneously and as part of the validation workflow. The goal of this test was to ensure that the firewall product does not prevent malicious traffic at the expense of operational accuracy.

AT&T Dynamic Defense was tested for operational accuracy under real-world scenarios throughout the entire test cycle, and Table 2 above showcases that it resisted false positives throughout testing.

Reporting and Logs

Dynamic Defense provides detailed insights into network traffic, tracking top talkers, blocked URLs, and applications. It supports threat identification, compliance monitoring, and security optimization with data filtering for targeted analysis. Logs can be filtered by time, IP, and actions and exported in multiple formats (Excel, CSV, JSON).

Usability

AT&T Dynamic Defense's Portal offers a user-friendly experience. The overview displays a network activity graph with blocked/allowed traffic and easy filtering options. Policy Management allows efficient security policy management, including geo-filtering, web filtering, and IP control. Insights combine reporting with traffic control, enabling direct actions from reports.

Smart Protection

AI-driven policy generation feature that monitors network traffic for 7 days, then automatically generates a tailored policy, simplifying management with minimal human intervention while ensuring strong protection.

Operational Efficiency Validation

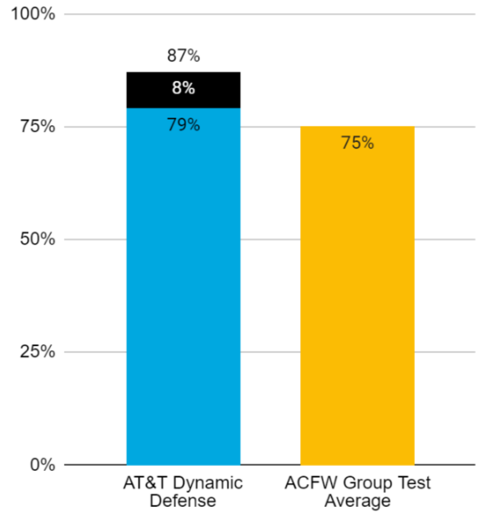

Figure 4. AT&T Operational Efficiency Comparison with Group Average from Recent Public Test

AT&T Dynamic Defense's operational efficiency measures the tested operating burden and complexity of setup and use. As such, the Operational Efficiency Rating measures both the ability of AT&T Dynamic Defense to detect and respond to cyber-attacks appropriately and ease of use. The operational efficiency was evaluated over the 12 categories listed in Table 4.

Figure 4 illustrates the comparison of Operational Efficiency Ratings between AT&T Dynamic Defense and the ACFW group average. AT&T Dynamic Defense starts with a baseline Operational Efficiency Rating of 79%. Moreover, the integration of AI-driven policy generation enhances this rating by an additional 8%. Furthermore, the firewall's capability to operate effectively out of the box, without requiring any configuration changes, significantly contributes to its improved operational efficiency.

CATEGORIES	AT&T	ACFW Group Test Average
Security policy configuration	High	Medium
Security Policy Management	Low[2]	Medium
Asset Management	Low[2]	Medium
Access Control	High	High
Compliance Management	High	High
Business Continuity Management	High	Medium
Risk Assessment & Mitigation	High	High
Security Metrics Reporting	High	High
Backup & Restore	High	Medium
Analytics	High	Medium
Customer Support	High	High
License Management	High	High

Table 3. AT&T Dynamic Defense vs ACFW Vendors Operational Efficiency Per Category

The features and functions within each category are awarded scores (integers 0 – 10) based on their capabilities. These scores are then tallied together to form a rating of high, med, or low. The Operational Efficiency Rating is equal to the total number of points scored respectively by the AT&T Dynamic Defense operational efficiency validation over the total number of points. Category ratings were awarded by averaging the scores within a category and using the following criteria:

- 🟩 High or Yes (Green) = 7 - 10 Points
- 🟨 Med (Yellow) = 4 - 6 Points
- 🟧 Low (Orange) =1 - 3 Point
- 🟥 NA/No (Red) = 0 Points

Conclusion

AT&T Dynamic Defense is an easy-to-deploy, AI-enhanced security solution that performs exceptionally well in detecting and blocking cyber threats. It provides an excellent defense-in-depth strategy for small to medium-sized businesses, simplifying network protection with AI-driven policy suggestions. The firewall's ability to detect attacks and mitigate threats before they reach the internal network makes it a valuable tool for businesses looking to improve their cybersecurity posture.

Methodology

The validation process included tests in a simulated environment based on common small and medium business (SMB) network configurations. The methodology focused on real-world attack scenarios, including spyware, APTs, malicious URLs, data exfiltration, and post-exploitation activities. The use of AI-driven policy generation was evaluated, and the system's operational efficiency was tested based on ease of use, deployment, and management. Please see the full report here for a more detailed description of the methodology.

[2] AT&T reports that these categories are on the roadmap for enhancements.