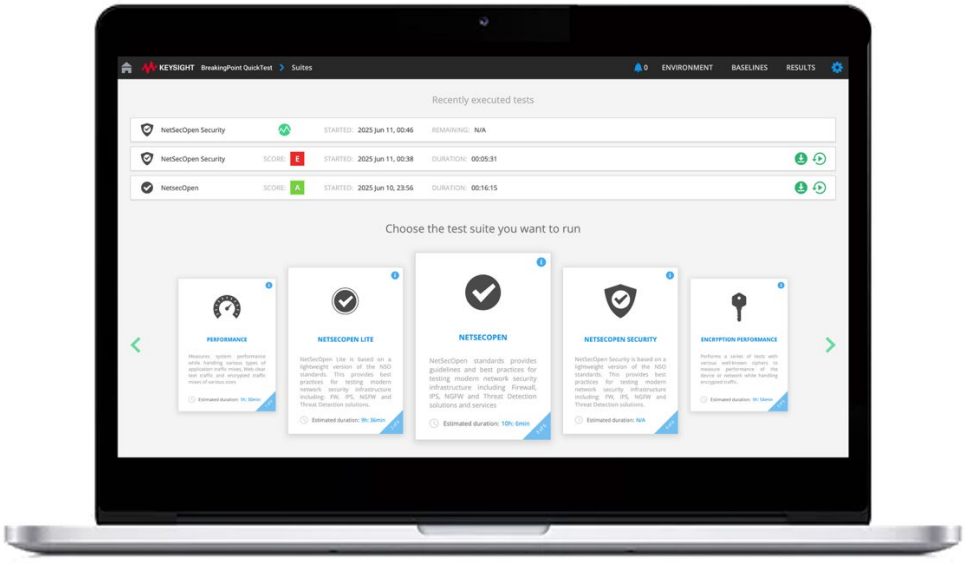
BreakingPoint QuickTest — Turn-Key Performance and Cybersecurity Testing

Problem: Complexity of Cybersecurity Testing

A properly conducted cybersecurity assessment provides details about network or device performance while handling traffic of varying complexity — from basic Layer 2-3 traffic to complex application mixes blended with the latest threat vectors. Similarly, a deep security-effectiveness assessment requires a combination of threat vectors and evasion techniques to accurately gauge an infrastructure's ability to detect, filter, and block different types of attacks. This validation is critical to ensuring a high-performing and secure network.

However, many organizations do not perform these assessments on a regular basis because the tools capable of such testing are too complex, network configuration changes are too frequent, or they lack staff with the knowledge required to effectively analyze test results.



KEYSIGHT

Highlights

- Simplified user interface that enables execution of complex test cases in just two to three clicks
- Pre-populated, problem-based test methodologies covering the top performance and security test scenarios
- A self-stabilizing, goal-seeking algorithm assess performance and security of a variety of infrastructures while reducing time to insight
- Expert analysis of each test run with actionable insights and results-based recommendations
- Continuously updated test suites that ensure relevant, real-world based assessments
- Ability to use both BreakingPoint and BreakingPoint QuickTest on a single test platform

Solution: Turn-Key Tests Designed to Accelerate Testing and Reduce Learning Curve

BreakingPoint QuickTest simplifies application performance and security-effectiveness assessments by providing individual test methodologies based on the type of test needed. Test suites include NetSecOPEN, NetSecOPEN Security, Performance, Encryption Performance, and Security. These easy-to-use test methodologies leverage the ongoing research from our global Application and Threat Intelligence (ATI) team and the many years of experience Keysight engineers have in testing various application and security devices and networks. The test suites employ powerful stabilization and goal-seeking algorithms that ensure accurate assessment of a diverse set of devices and systems, and expert analysis that delivers actionable insights after each test run.

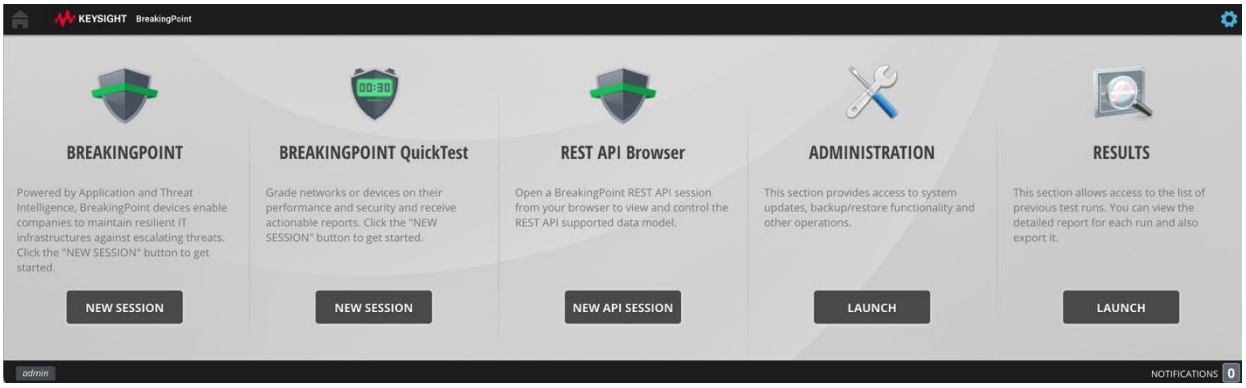
BreakingPoint QuickTest delivers all the power of our industry-leading BreakingPoint, enabling organizations to optimize the speed and efficacy of their cybersecurity testing without compromise.

Key Features

- Pre-populated, turn-key test suites simplify complex test scenarios and reduce time to insight
- Self-adjusting, goal-seeking algorithms designed to work in varied environments
- Every assessment is followed by a report with actionable observations and recommendations
- Continuously updated suites and categories to cover new and emerging scenarios

Product Capabilities

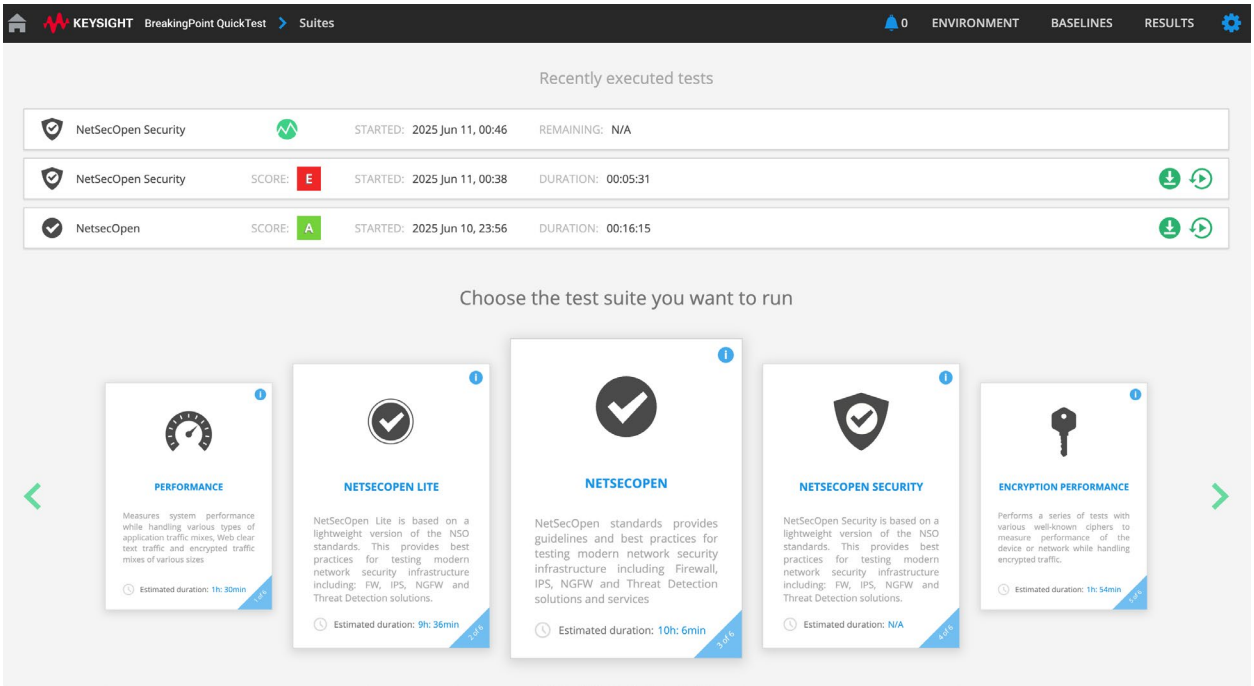
A simplified user interface ensures a short learning curve for both new and existing BreakingPoint customers. BreakingPoint QuickTest is available in the same web application framework (WAF) used to access the BreakingPoint chassis.



BreakingPoint QuickTest sign in screen

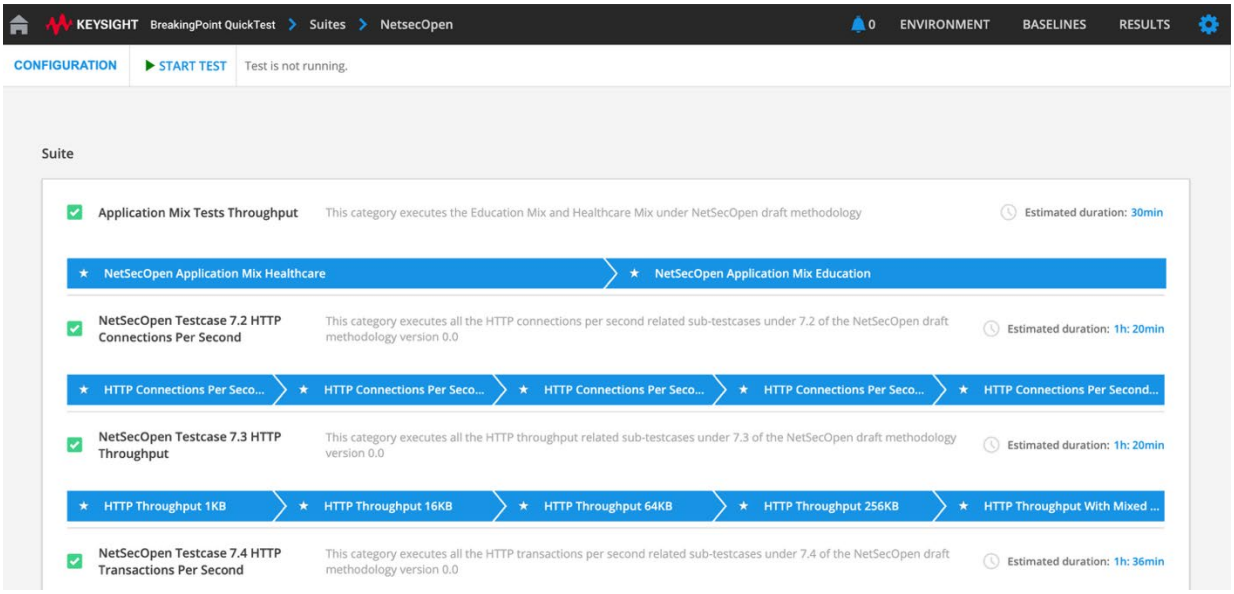
Pre-packaged traffic profiles with adjustable load

After the users are signed in, they see their recently executed test runs and the available, turn-key test methodology suites. For example, the ‘NetSecOPEN’ test suite runs a series of real-world application mixes as well as HTTP and HTTP performance tests to characterize the performance aspects of any system or device under test (SUT or DUT). Similarly, the ‘NetSecOPEN Security’ test suite will run various types of attacks like exploits, malware, and evasions to accurately measure the security efficacy of a DUT / SUT in detecting and blocking attacks.



BreakingPoint QuickTest welcome screen showcasing recent test runs and available test suites

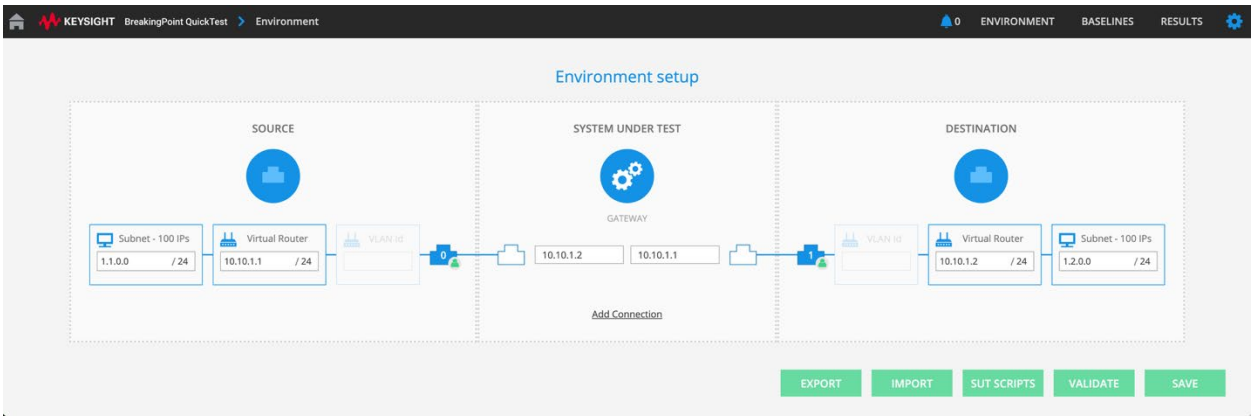
Within each test suite there are several categories of assessments that users can select. The carefully designed user interface (UI) ensures that most of the complex decision making has been packaged so users can run any of the pre-canned suites with minimal clicks. For example, the 'NetSecOPEN' suite uses the NetSecOPEN Healthcare and Education application mixes which are usually complex to configure, as well as RFC9411 HTTP and HTTPS performance tests which can be time consuming to run and stabilize over various environments. However, with BreakingPoint QuickTest, you can qualify your network infrastructure's performance and compliance with a click of a button.



Upon selecting any of the suites, users select the types of traffic to use in the test

Error-free environment setup

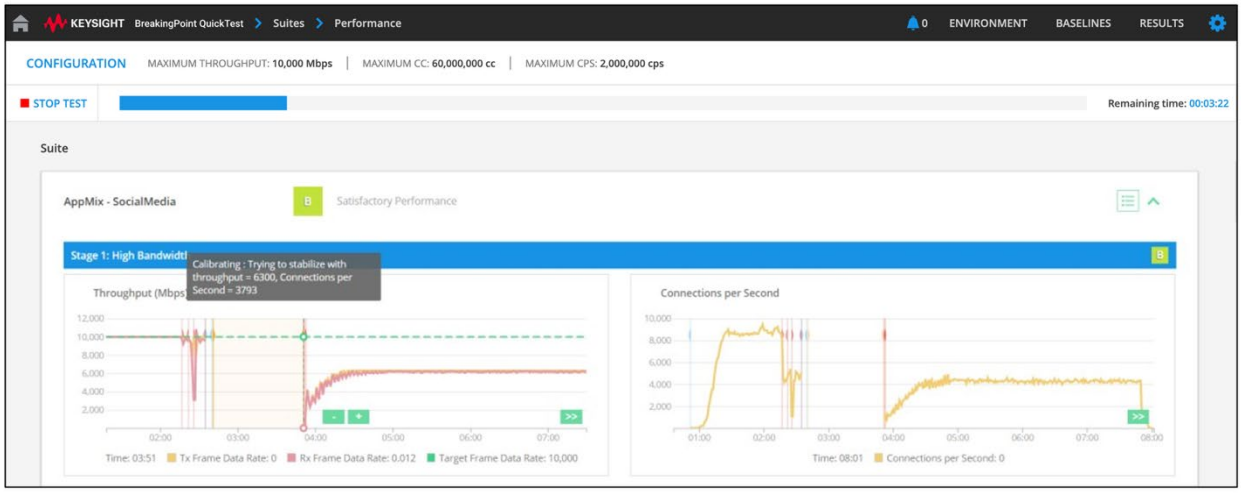
Simplicity is the theme of BreakingPoint QuickTest, which is also reflected in the environment setup where the user can configure the IP addresses for the test tool simulating a client ‘source’ and server ‘destination,’ and the DUT gateway all in one page. The ‘Validate’ button validates port / traffic connectivity, further reducing debug cycles usually spent in figuring out traffic connectivity.



A graphical form-fill simplifies how users connect the traffic generator test system to the SUT / DUT

Intelligent stabilization / calibration

Each suite comes with a stabilization / calibration algorithm that handles a diverse setup of traffic conditions and finds the optimum performance / security results of these environments accurately. By continuously assessing for failure points and recalibrating the test, BreakingPoint QuickTest challenges the system or device under test to its breaking point, but then automatically adjusts the load to maintain the peak throughput for the test duration.



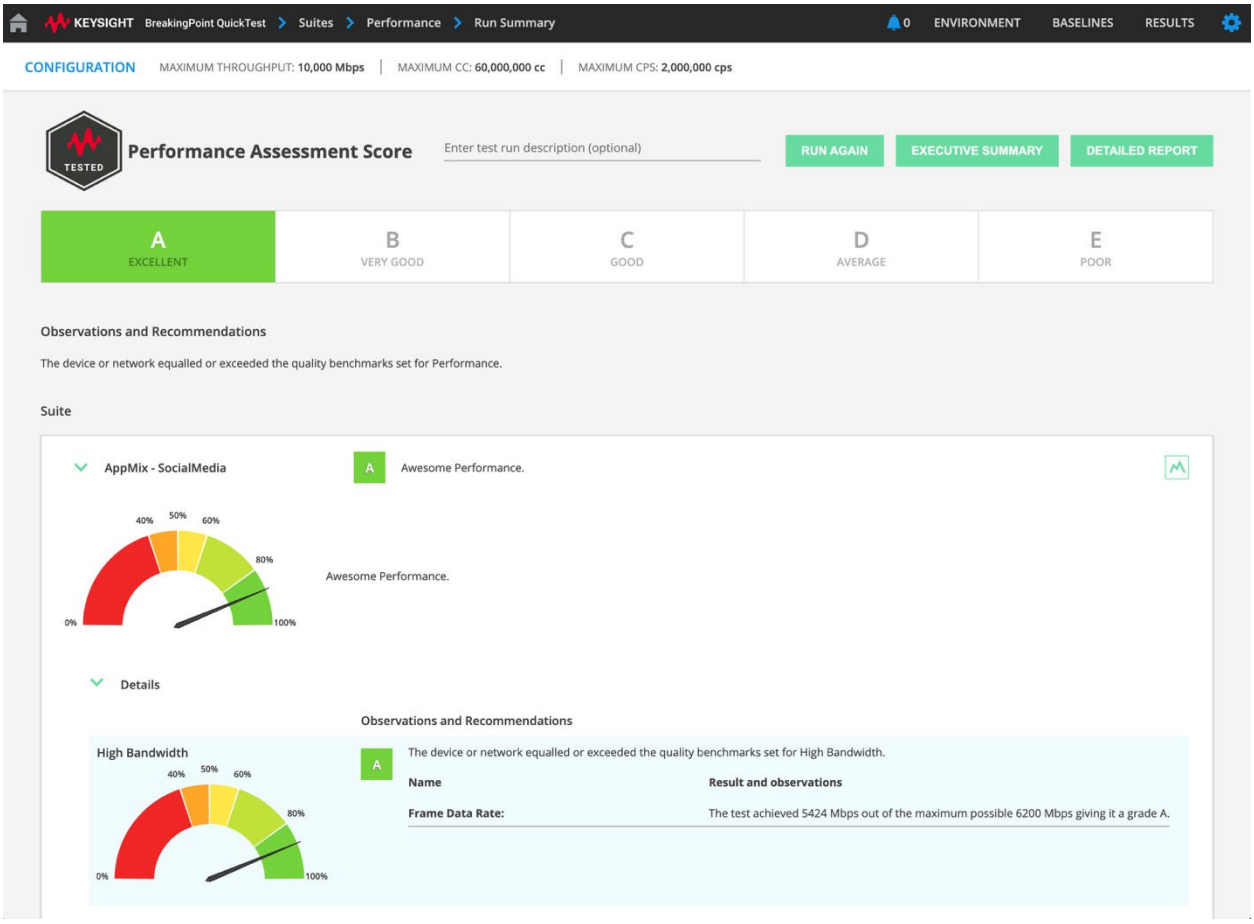
BreakingPoint QuickTest runs showcasing the stabilization and calibration algorithms

Reports and actionable performance scores

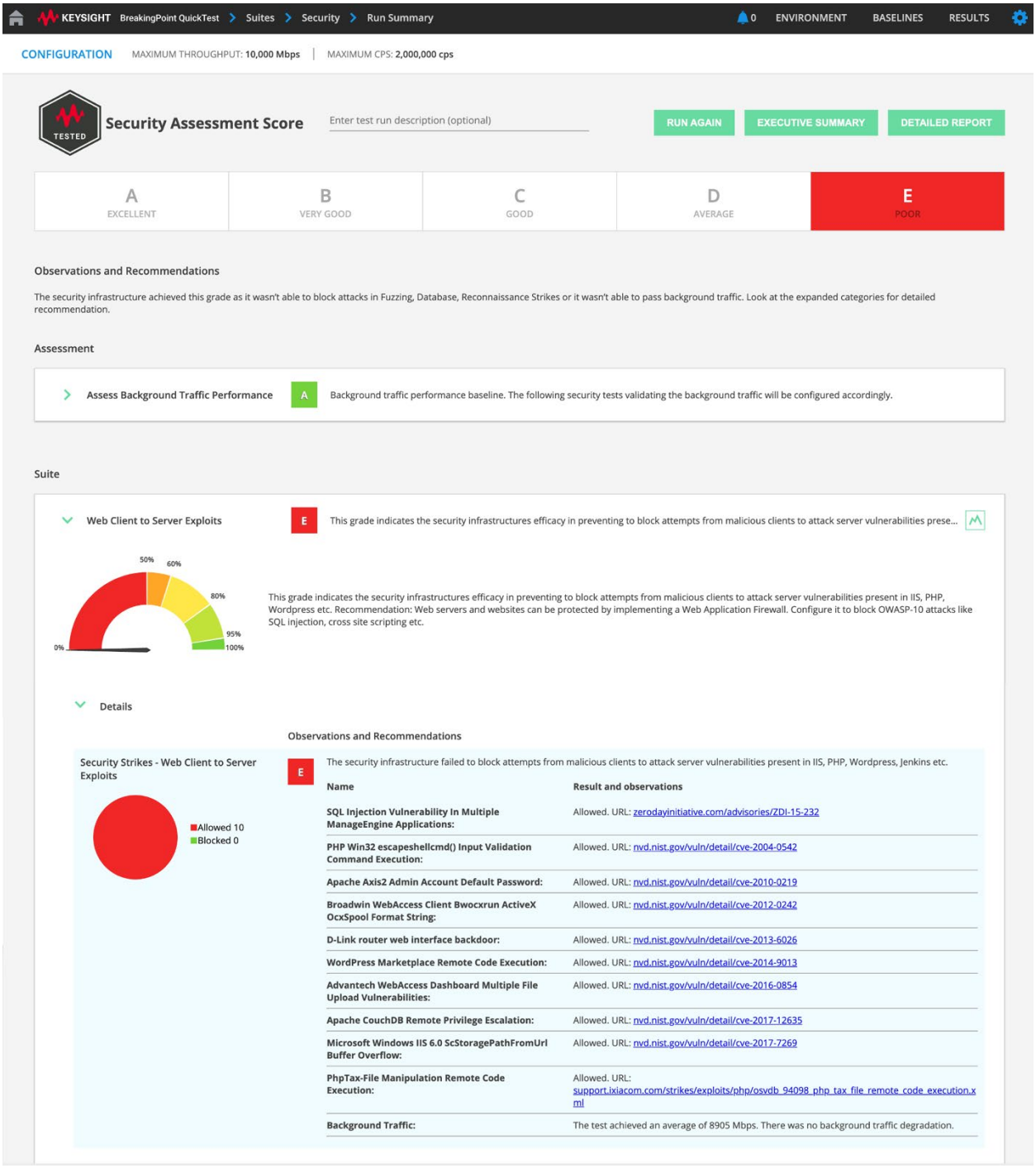
After the test concludes, the report and results have actionable grades and insights that can help users:

1. Understand the ‘real’ performance of their SUT / DUT
2. Take corrective actions based on results and the actionable insights provided
3. Evaluate the impacts of change management by comparing before and after scenarios
4. Gain more flexibility beyond that offered in BreakingPoint QuickTest by selecting the option to move to BreakingPoint classic for features like our rich network neighborhood, configuration and editing of application mixes, and creation of customized tests

The test reports have a high-level synopsis that provides overall scores for the entire suite based on the weighted average of each of the categories and scores for each individual category so users can get more in-depth insights. Apart from scores, the reports also have actionable observations and recommendations.



BreakingPoint QuickTest Performance Assessment results and reports showing grade of the suite and individual categories



BreakingPoint QuickTest Security Assessment results and reports showing grade of the suite and individual categories

Specifications

Suite	Categories
Performance	• **AppMix – Business**: A mix of popular enterprise productivity tools and business applications; includes Office 365, Salesforce, Webex • **AppMix – SocialMedia**: A mix of popular social media applications prevalent in enterprise environments; includes Twitter, Facebook, YouTube • **AppMix – Enterprise Datacenter**: A mix of popular datacenter applications; includes Oracle, SMB, Citrix, HTTPS • **Web Clear Text – Mix Traffic Performance**: Download and upload of a mix of small to large clear text web pages • **Web Encrypted – Mix Traffic Performance**: Download and upload of a mix of small to large web pages that are encrypted with popular ciphers
Security	• **Assess Backgroud Traffic Performance:** Automatically discovers the best application traffic parameters and configure them as background for subsequent security tests • **Web Client to Server Exploits:** A collection of the latest critical and high severity exploits that a malicious client may use against vulnerable services • **Web Server to Client Exploits:** A collection of the latest critical and high severity exploits that a malicious server may use to infect a vulnerable web client • **Critical Exploits – Multiple Variants:** A collection of multiple, critical client and server exploits • **Email Vulnerabilities:** A collection of exploits that target vulnerabilitites present in popular email clients and servers • **Dangerous Attachments:** Client attempts to upload potentially dangerous file types encapsulated in Zip, RAR, etc to SMTP server • **Evasions Efficacy:** Run strikes that attack services with and without evasions to check security infrastrcuture's ability to block evasions • **File Server Attacks:** Simulates exploits that target file servers • **Botnets:** Simulates command and control communications from a collection of botnets • **Malware:** Sends a collection of Win32 and iOS malware • **Denial of Service:** Performs denial of service attacks against services and operating systems • **Database:** A collection of exploits that targets vulnerabiitites in database servers • **Reconnaissance Strikes:** A collection of critical response exploits that a malicious client would use against vulnerable servers • **Fuzzing:** Includes a collection of protocol fuzzers that attempt to scramble and crash various protocols
NetSecOPEN	• **NetSecOPEN Application Mix Tests Throughput**: Executes the NetSecOPEN Education and Healthcare Application Mix tests • NetSecOPEN 7.2 HTTP Connections Per Second: Executes all NetSecOPN HTTP connections per second test cases as outlined under RFC9411 section 7.2 • NetSecOPEN 7.3 HTTP Throughput: Executes all NetSecOPEN HTTP throughput test cases as outlined under RFC9411 section 7.3 • NetSecOPEN 7.4 HTTP Transactions Per Second: Executes all NetSecOPEN HTTP transaction per second test cases as outlined under RFC9411 section 7.4 • NetSecOPEN 7.5 HTTP Concurrent Connections: Executes all NetSecOPEN HTTP concurrent connections test cases as outlined under RFC9411 section 7.5.

Suite	Categories
	• NetSecOPEN 7.6 HTTPS Connections Per Second: Executes all HTTPS connections per second test cases as outlined under RFC9411 section 7.6 • NetSecOPEN 7.7 HTTPS Throughput: Executes all HTTPS throughput connections per second test cases as outlined under RFC9411 section 7.7 • NetSecOPEN 7.8 HTTPS Transactions Per Second: Executes all HTTPS transactions per second test cases as outlined under RFC9411 section 7.8 NetSecOPEN 7.9 HTTPS Concurrent Connections: Executes all NetSecOPEN HTTPS concurrent connections tests as outlined under RFC9411 section 7.9
Encryption performance	• TLSv1.2 RSA AES 128 GCM SHA256: Runs concurrent connections, connections per second, and throughput tests to find the maximum performance of the DUT with cipher configuration version TLS 1.2, key exchange RSA, bulk cipher AES 128 GCM SHA256, key size 2K • TLSv1.2 ECDHE RSA AES 128 GCM SHA256: Runs concurrent connections, connections per second, and throughput tests to find the maximum performance of the DUT with cipher configuration version TLS 1.2, key exchange ECDHE RSA, bulk cipher AES 128 GCM SHA256, key size 2K • TLSv1.2 ECDHE ECDSA AES 128 GCM SHA256: Runs concurrent connections, connections per second, and throughput tests to find the maximum performance of the DUT with cipher configuration version TLS 1.2, key exchange ECDHE ECDSA, bulk cipher AES 128 GCM SHA256, key size 2K • TLSv1.3 ECDHE ECDSA CHACHA20 POLY1305 SHA256: Runs concurrent connections, connections per second, and throughput tests to find the maximum performance of the DUT with cipher configuration version TLS 1.3, key exchange ECDSA, bulk cipher CHACHA20 POLY1305 SHA256, key / curve size 256-P curve • TLSv1.3 ECDHE ECDSA AES 256 GCM SHA384: Runs concurrent connections, connections per second, and throughput tests to find the maximum performance of the DUT with cipher configuration version TLS 1.3, key exchange ECDHE ECDSA, bulk cipher AES256 GCM SHA384, key / curve size 256-P curve • TLSv1.3 ECDHE ECDSA AES 128 GCM SHA256: TLSv1.3 ECDHE ECDSA AES 256 GCM SHA384: Runs concurrent connections, connections per second, and throughput tests to find the maximum performance of the DUT with cipher configuration version TLS 1.3, key exchange ECDHE ECDSA, bulk cipher AES128 GCM SHA256, key / curve size 256-P curve
NetSecOPEN security	• NetSecOPEN Evasions: Tests the ability of a DUTs IPS and IDS engines to detect and block known FTP, HTTP, IP, TCP and URL based CVEs that been obfuscated to bypass detection as outlined in the NetSecOPEN Security test suite • NetSecOPEN Malware: Tests the ability of the DUTs IPS and IDS engines to detect and block a wide variety if malware variants as outlined in the NetSecOPEN Security test suite • NetSecOPEN Vulnerabilities: Tests the ability of the DUTs IPS and IDS engines to detect and block a wide variety of CVEs as outlined in the NetSecOPEN Security test suite

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

KEYSIGHT

This information is subject to change without notice. © Keysight Technologies, 2019 – 2025, Published in USA, August 5, 2025, 7019-0130.EN