BreakingPoint®—Applications and Security Testing

Validate the security posture of your networks with real applications and a complete range of threat vectors.

PROBLEM: REAL-TIME CHALLENGES FOR REAL-WORLD TESTING

These days, organizations rely on a wide variety of security solutions to protect their networks from cyber-attacks and traffic anomalies. But the more tools deployed, the more complex a security infrastructure becomes. The result: a hodgepodge of security solutions that are tough to verify and challenging to scale. Worse yet, these complex system interactions pose a serious risk to security performance and network resiliency.

SOLUTION: AN EASY-TO-USE TESTING ECOSYSTEM FOR MODERN NETWORK NEEDS

To counter such challenges, businesses require an application and security test solution that can verify the stability, accuracy, and quality of networks and network devices.

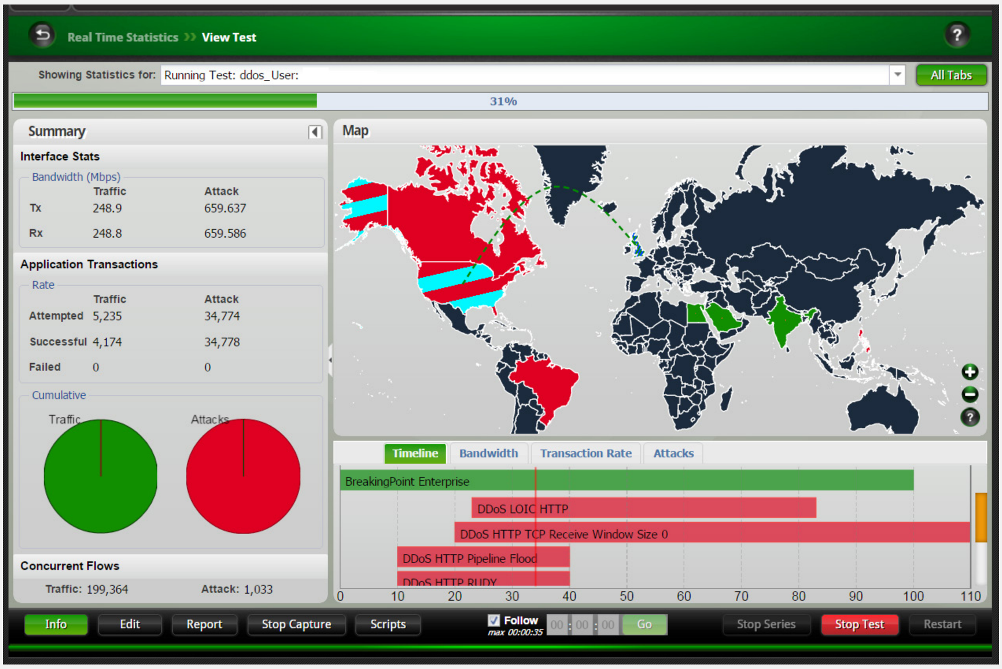
Enter BreakingPoint. By simulating real-world legitimate traffic, distributed denial of service (DDoS), exploits, malware, and fuzzing, BreakingPoint validates an organization's security infrastructure, reduces the risk of network degradation by almost 80%, and increases attack readiness by nearly 70%.

How might a particular configuration or security setup withstand a cyber-attack? BreakingPoint addresses that by simulating both good and bad traffic to validate and optimize networks under the most realistic conditions. Security infrastructures can also be verified at high-scale, ensuring ease of use, greater agility, and speedy network testing.

ixia
A Keysight Business

HIGHLIGHTS

- Measure and harden the performance of network and security devices
- Validate network and data center performance by recreating busy hour Internet traffic at scale
- Stress network infrastructures with 37,000+ security attacks, malware, botnets, and evasion techniques
- Find network issues and prepare for the unexpected with the industry's fastest protocol fuzzing capabilities
- Emulate sophisticated, large-scale DDoS and botnet attacks to expose hidden weaknesses
- Ensure the always-on user experience
- Train staff by simulating highly realistic cyber-range/training environment
- Validate service provider networks using emulations over 3G/4G/LTE
- Amplify test traffic realism by running TrafficREWIND summary configurations that replicate the dynamic nature of production networks and applications



Showing Statistics for: Running Test: ddos_User:

Interface Stats

Bandwidth (Mbps)

	Traffic	Attack
Tx	248.9	659.637
Rx	248.8	659.586

Application Transactions

Rate

	Traffic	Attack
Attempted	5,235	34,774
Successful	4,174	34,778
Failed	0	0

Concurrent Flows

Traffic: 199,364 Attack: 1,033

Leverage extensive automation and wizard-like labs that address many use-case scenarios, including validation of lawful intercept and data loss prevention (DLP) solutions, RFC2544, DDoS (shown), Session Sender, and Multicast. In addition, a REST and TCL API help you build and execute automated tests.

KEY FEATURES

- Simulates 300+ real-world application protocols
- Allows for customization and manipulation of any protocol, including raw data
- Generates a mix of protocols at high speed with realistic protocol weight
- Supports 37,000+ attacks/malwares
- Delivers from a single port all types of traffic simultaneously, including legitimate traffic, DDoS, and malware
- Bi-monthly Application and Threat Intelligence (ATI) subscription updates ensure you're are current with the latest applications and threats
- Combined with the CloudStorm™ platform, BreakingPoint reaches a staggering performance with a fully-populated chassis—2.4 Tbps / 1.44 billion sessions and 42 million connections per second—to emulate enterprise-wide networks to continent-scale mobile carrier networks