

## I D C V E N D O R S P O T L I G H T

---

# The Inevitable Failure of Content-Aware/DPI Network Devices — and How to Mitigate the Risk

September 2008

Adapted from *Worldwide Network Test and Measurement 2008–2012 Forecast and 2007 Market Shares* by Elisabeth Rainge, IDC #211881

Sponsored by [BreakingPoint Systems](#)

---

*Organizations are increasingly reliant upon the performance, security, and availability of networked applications to achieve business goals. At the same time, the growing popularity of latency-sensitive, bandwidth-heavy applications is placing heavy demands on network infrastructures. Faced with these demands and increasingly sophisticated security threats, network equipment providers (NEPs) and telecommunications service providers (SPs) have delivered a new generation of high-performance, content-aware network equipment and services.*

*Content-aware devices that leverage deep packet inspection (DPI) functionality have been around for more than seven years, and new content-aware 10 gigabit, 40 gigabit, and higher performance equipment is coming to market each year. However, recent high-profile performance and security failures are bringing renewed focus to the importance of sufficient testing to ensure content-aware network devices can perform under real-world and peak conditions.*

*Today's sophisticated and complex high-performance network devices and the network they run on require a more comprehensive approach to testing prior to deployment than traditional testing tools are able to provide. NEPs, SPs, and other organizations require testing solutions capable of rigorously testing, simulating, and emulating realistic application workloads and security attacks at line speed. Equally important, these testing tools must be able to keep pace with emerging and more innovative products as well as thoroughly vet complex content-aware/DPI-capable functionality by emulating a myriad of application protocols and other types of content at ever-increasing speeds and feeds to ensure delivery of an outstanding quality of experience (QoE) for the customer and/or subscriber. This paper examines the major drivers and requirements for this new category of testing tools. It also looks at the solutions offered by application performance and security testing vendor BreakingPoint Systems to address the requirements of this strategically significant market.*

## Introduction

Network infrastructures today are built on IP foundations. However, measuring and managing application performance in relation to network devices remain challenges. To make matters worse, content-aware networking mandates controls for Layers 4–7 as well as the traditional Layer 2–3 attributes. Yet, to date, the bulk of the IP network testing industry has focused primarily on testing of Layers 2–3 with minimal consideration for Layers 4–7. Now with the rise of content-driven services, Layers 4–7 are increasingly strategic areas for network optimization and bulletproofing.

Even as NEPs and SPs rush to introduce newer, more sophisticated content-aware/DPI-capable devices to reap the associated business and recreational benefits these products deliver, the testing of these devices has remained stagnant. Legacy testing solutions and traditional testing practices

typically focus on the IP network connection, especially routers and switches, and do not have sufficient functionality or capability to properly test this new class of devices. Nor are they aligned with content-driven approaches such as using and applying test criteria using stateful blended traffic and live security strikes at line speeds. The introduction of content-aware functionality into the network drives many new variables for testing that resist corner-case approaches and instead require realistic, randomized traffic testing at real-time speeds. The inability to test this new set of content-aware and software-driven packet inspection devices contributes to the deployment challenges and potential failure of many of them once they are deployed.

A key consideration for NEPs and SPs is the recent introduction of a new generation of testing tools that enable accurate performance and security testing of content-aware/DPI-capable devices. Content-aware network equipment has the ability to adapt to new network requirements and technologies as they appear, prioritize traffic for business and recreational purposes, and better secure the network from malicious attacks. Subsequently, network testing tools must have the ability to test using stateful Layer 4–7 application traffic blended with live security strikes. The new generation of testing tools also means new testing rules are being used by NEPs and SPs to ensure content-aware/DPI-capable devices perform correctly prior to their live deployment. These rules include testing of content-aware devices using the following criteria:

### ***Application Traffic***

Natively generated application traffic using a variety of different application protocols running at network speeds in the multigigabit range can tax the performance and security capabilities of the network and/or networked devices. For network infrastructures that must handle many more applications, with increasingly greater levels of sophistication, stress testing of both the network and load in combination is important. This approach helps ensure that, once deployed, the devices are able to recognize traffic patterns and cope with changing (and challenging) business and recreational situations.

### ***Live Security Strikes***

Many of today's NEPs, SPs, and largest corporations require advanced testing solutions capable of detecting vulnerabilities before a security breach shuts down their operations or a service provider's network and severely impacts their ability to do business. Live security attacks coupled with realistic, sophisticated business application traffic are needed to properly test and certify network devices can perform well against the global barrage of increasingly more sophisticated security and denial of service attacks. Another reason this is necessary is because IP networks lack the security inherent in older telecommunications infrastructures.

### ***Testing at Line Speed***

Traditional network testing technologies are not optimized for fast, heavy transactional environments. This creates a demand for modern testing tools that can handle a variety of types of application traffic and operate at very high transactional speeds. As more data traffic flows over the network due to streaming video, music downloads, and other content-based services, network behavior is changing. The mix of the stress on the network can come from combinational services of voice, video, and data traffic. Further, the increasing mobility of users — whether the access type is WiFi, cellular, or broadband — fuels different usage patterns due to time of day or roaming privilege requirements. This new class of testing technology lets companies develop and run test cases that include a realistic combination of application traffic and multiple applications while maintaining speeds equal to or in excess of multigigabits. Since data network (IP network) traffic drives far greater volumes of transactions across the service provider's infrastructure, it is difficult to accurately test for the realities of the typical loads and traffic that these systems regularly process without deploying this type of testing.

As new technologies emerged or network infrastructures changed, ordinary testing tools had to be updated and/or rewritten. Testing network devices for application performance using software development testing methods provides one required attribute, while testing Layer 2–7 hardware performance provides another view on infrastructure reliability. But it is the combination of the software competency with the hardware competency that has remained elusive to suppliers of testing tools as well as their customers. A key issue has been the relatively stronger need of network staff or applications staff to test the infrastructure from their perspective. However, as the overall IT and communications infrastructures have matured and content-based traffic continues to grow exponentially, the blended view is increasingly critical.

Organizations can benefit from deploying the type of testing tools with enough capability and flexibility to test and work with new network technologies and content-aware/DPI-capable devices as they appear without first having to be completely redesigned.

Finally, the focus of testing cannot be confined exclusively to content-aware/DPI-capable devices. Careful consideration must be given to testing the hardware complexities and highly customized software features when rolling out new carrier-grade equipment because these factors further complicate the testing processes. For instance, efforts to drive product differentiation are frequently hampered by requirements to deliver a competitive product and/or innovative features within six to 12 months or less, even though significantly more time is required to validate and formally accept any new network hardware. Good testing not only can make the competitive difference when encountering this type of dichotomy but in many cases may mean the difference between deployment success or failure.

## **The Benefits of Advanced Realistic Testing Tools**

For those organizations that decide to use this new breed of testing tools, many benefits accompany the ability to test a broad range of applications running on a variety of technologies at high speeds and heavy network traffic. First, the testing tools are far more likely to quickly and accurately detect what normally would be hard-to-find problems associated with function, performance, or security weaknesses. Second, they can accelerate time to market and development time by catching potential problems quickly and thereby reduce R&D costs.

Testing with this degree of thoroughness also mitigates the risk of performance or security issues in the final production environment. It ensures more effective testing of networks and networked devices in complex and dynamic environments because the tools make it possible to simulate realistic converged application traffic with high session counts delivered at line speed. In addition, they also allow device manufacturers to accurately test and determine whether their new devices can meet the application traffic requirements of NEPs and SPs.

Since testers can accurately recreate the scenarios that duplicate real-world conditions, it is possible to create core applications such as messaging and collaboration. These applications can be extended and blended to create applications such as unified communications, or even more innovative applications. Additionally, organizations can use these testing capabilities to test firewalls, intrusion prevention systems (IPS), load balancers, and other content-aware technology products as well as mission-critical, high-performance operating environments. With multigigabit speeds, organizations can run millions of TCP sessions while simultaneously blocking live security attacks. In a network environment dominated by content-aware/DPI-capable devices, the ability to measure accurate performance no longer is a pure case of speed; rather, it's performance in the face of millions of TCP sessions. Measurement of content-aware/DPI-capable device performance is accurate only when mirroring actual real-world use, which in a network environment equals TCP sessions.

## Market Trends

The network test and measurement market reached \$5.3 billion in 2007 and is expected to increase at a CAGR of 9.0% to reach \$8.2 billion in 2012. The requirement for innovative, agile test and measurement solutions remains a high priority for NEPs and SPs to validate the performance capabilities of a network prior to live operational deployments. Growth in this segment will continue to reflect the strength of NEP and SP technology investments along with trends such as the migration of content-aware/DPI-capable devices contributing to the growth of this market.

The network industry is evolving product architectures to support virtualization strategies and scalable, distributed designs at a time when SOA concepts and constructs are seeping into the newest network architectures and operating systems and the network equipment software assets are starting to be exposed as services. Concurrently, most mobile networks and other value-added infrastructures are moving toward commercial servers and away from proprietary black-box implementations. This suggests that testing is poised to move from entirely customized to more standardized solutions.

Additionally, streamlined spending by NEPs indicates they may be in the process of gaining the kinds of efficiencies that will ensure their longevity. However, this will entail realigning the culture of the product development and testing staff to persuade them to embrace commercial and scripted product solutions and convince developers that it's not necessary to write a new script each time they code. As the market matures, testing equipment must keep pace with innovative products and testing tools must be able to simulate and support these events at a minimum of 10 gigabits or faster.

## Considering BreakingPoint Systems

BreakingPoint Systems was founded in 2005 by experienced engineers who had been developing high-speed networking devices and had recognized a need for a new class of network and application testing tools capable of realistically simulating an enterprise network environment to facilitate the development of high-performance, reliable products. The company's products focus on application, performance, and security testing for content-aware devices; support realistic traffic generation at multigigabit speeds; and can accommodate millions of connection setups per second of traffic testing. These capabilities make BreakingPoint's products attractive to NEPs, SPs, and other organizations that use them to accelerate the development of high-performance networks and network devices.

The company provides many of the testing components required by most network OEMs and NEPs "out of the box." BreakingPoint solutions are architected in three independent layers that work together to simulate realistic applications. BreakingPoint also claims to offer the following competitive advantages:

- **Fast.** BreakingPoint has a solution that can deliver realistic application traffic and live security strikes at 20Gbps in a single 4U chassis scaling easily to 200Gbps+ speeds.
- **Accurate.** BreakingPoint comes out of the box with 60+ applications and 3,600+ live security strikes, combined with the ability to accelerate proprietary application traffic.
- **Easy to use.** Intuitive management interface, application profile repository, multiuser capabilities, and extensive automation improve productivity and reduce time to test.
- **Flexible.** Flexible architecture has the ability to add custom application protocols and security attacks, mix 1GbE and 10GbE interfaces, and scale to support large testing environments.
- **Responsive.** BreakingPoint introduces new application protocols and security strikes weekly, and custom applications are created in less than a day.

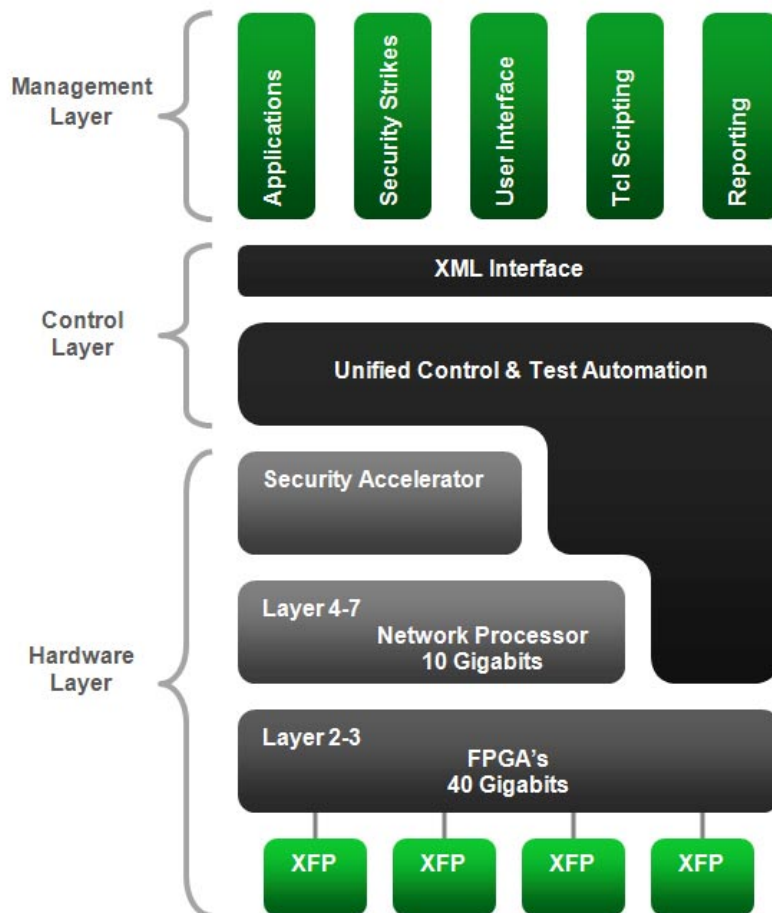
Designed as an all-in-one box that provides multiport and multiuser capabilities, BreakingPoint's patent-pending testing solution deploys quickly, automates tests, and controls the device being tested, as shown in Figure 1. The company also offers an extensive library of preconfigured tests that users can emulate, enhance, and integrate with their own testing components.

Multiple field programmable gate arrays (FPGAs), network processors, and an array of embedded processors produce millions of real application data streams resulting in enhanced security testing capability. The company also makes the following performance claims:

- 15 million simultaneous TCP sessions
- 1.5 million TCP/IP requests per second
- 20Gbps of stateful application traffic
- 80Gbps of Layer 2–3 traffic (scales to 200Gbps)
- Supports transmissions and verification of up to 60 million packets per second at 64-byte packets

**Figure 1**

BreakingPoint Architecture



Source: BreakingPoint Systems, 2008

## **Challenges**

BreakingPoint initially experienced financial and operational growth as a start-up, achieving a 106% increase in revenue and a 150% increase in new customers while growing headcount by 28%. The company's current challenges now revolve around growing its customer base. Because the majority of the network test market is concentrated in the hands of a few large vendors, BreakingPoint must maintain its agility and focus. In the coming five years, BreakingPoint will have to compete for business within the R&D and QA groups of companies of leading NEPs. The company will primarily focus on NEP R&D labs and then on telecom and cable R&D labs.

Within three years, IDC believes that BreakingPoint will work toward serving enterprise IT department needs for systems to monitor and manage the interplay of applications, security, and network traffic. This move will require careful strategic planning to be successful. Nevertheless, there is a good opportunity for this type of a solution within enterprise IT departments due to the evolution of management requirements for networked infrastructures and the relatively small number of network-based solutions available or in the works today.

## **Conclusion**

The introduction of content-aware functionality in network equipment significantly broadens the scope of testing requirements. From anticipating the issues of various teams within the IT and network departments to accepting the unpredictability of consumer demand for content, the testing and the traffic loads on network equipment have an ever greater set of variables. Adding security considerations and the unpredictability of malicious attacks to the mix drives complexity.

Historically, organizations have relied on good testing tools and even better security tools to protect their networks from malicious attacks. Until recently, there was no way to test both performance and security together using the same data and tests because NEPs and SPs were unable to generate a realistic mix of business, recreational, malicious, and proprietary application traffic at high enough speeds. The requirement for such a mix of content- and application-aware network infrastructure testing at high speeds has been largely unaddressed — until now. Improved solutions capable of addressing these deficiencies are finally emerging.

BreakingPoint's support for simulation of proprietary application traffic is an important step toward addressing the growing application-oriented and content-aware network test challenge. Today, BreakingPoint's products make it possible to do both performance and security testing, helping to accelerate product development.

IDC believes the market for network test and measurement automation will continue to grow in size and importance. To the extent that BreakingPoint Systems can address the challenges described in this paper, the company has a significant opportunity for success.

---

### **ABOUT THIS PUBLICATION**

This publication was produced by IDC Go-to-Market Services. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Go-to-Market Services makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

### **COPYRIGHT AND RESTRICTIONS**

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests, contact the GMS information line at 508-988-7610 or [gms@idc.com](mailto:gms@idc.com). Translation and/or localization of this document requires an additional license from IDC.

For more information on IDC, visit [www.idc.com](http://www.idc.com). For more information on IDC GMS, visit [www.idc.com/gms](http://www.idc.com/gms).

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 [www.idc.com](http://www.idc.com)