ixia

DATA SHEET

Harden Your Network Against Cyber Attacks

The Ixia BreakingPoint Storm™ is the world's first device to pinpoint previously impossible-to-detect stress fractures in your network, network devices, or data center before they are exploited

The Storm™ is designed for the world in which we live—a perilously interconnected universe with escalating network traffic and cyber attacks from a growing list of enemies. It allows you to pinpoint previously impossible-to-detect weaknesses and vulnerabilities in networks, network devices, and data centers before they are exploited to wreak havoc within critical network infrastructures.

Ixia BreakingPoint Provides a Virtual CT Scan for Your Network

Much as a medical computed tomography or CT scan requires the injection of dyes and the emission of waves of energy into the body, the BreakingPoint Storm™ radiates extreme applications and malicious traffic into network components such as routers, switches, firewalls, and servers and displays the effects over time. Based on network processor technology, the BreakingPoint Storm provides unprecedented insight by producing these real-world conditions:

- A custom blend of stateful application and malicious traffic at 40 Gigabits per second
- An always-current real-world mix of applications and attacks
- Unprecedented scalability, producing Internet-scale scenarios and traffic from millions of users

The BreakingPoint Storm provides this granular real-world simulation and is the only product capable of measuring the resiliency of switches, routers, firewalls, IPS devices, servers, networks, and data centers. By measuring the resiliency—performance, security, and stability—of discrete network components and data centers under high-stress, hostile conditions, BreakingPoint enables you to harden the resiliency of your critical IT infrastructures.

Key Benefits

- Harden networks by assaulting them with a custom, global, and current blend of stateful applications, live security attacks, and high stress load to probe every weakness and vulnerability
- Optimize data center resiliency by simulating the behavior of millions of users, real-world applications, and security attacks—all without deploying racks of high-speed servers and costly software
- Evaluate and select the most appropriate network equipment for critical infrastructure with standardized, repeatable, and deterministic product assessments
- Measure and harden the resiliency of router, switch, firewall, IPS, and UTM devices by subjecting them to real-world conditions prior to deployment and after patches or configuration changes
- Validate lawful intercept and DLP systems with multilingual "needle in a haystack" simulation
- Identify and remediate problem areas that require tuning and configuration changes
- Audit and maintain standards compliance throughout device life cycle
- Conduct research and train security experts with BreakingPoint's cyber range in a box, which re-creates Internet-scale network conditions and cyber threats
- Analyze the impact of traffic on network devices and systems to conduct research and train security experts

Stay Current with Comprehensive Applications, Attacks, Service, and Support

BreakingPoint also provides the BreakingPoint Application and Threat Intelligence (ATI)™ Program, an all-in-one service backed by a team of security experts, to complement the BreakingPoint Storm. This program keeps BreakingPoint products updated with the latest security attacks and applications, as well as new features and performance upgrades.

BreakingPoint Storm Features

Stress Networks, Data Centers, and Devices with Real-World Conditions to Pinpoint Stress Fractures

- Produces blended applications and current security attacks at global-scale while emulating millions of users
- Ships with more than 250 application protocols out of the box, including popular applications such as AOL® IM, Google® Gmail, FIX, Gnutella, IBM® DB2®, VMware® VMotion™, HTTP, Microsoft® CIFS/SMB, MAPI, Oracle®, Encrypted BitTorrent™, eDonkey, MSN® Nexus, RADIUS, SIP, Skype™, Windows Live Messenger
- Provides an optional Custom Application Toolkit and Custom Strike Toolkit to create and accelerate custom applications and security attacks
- Provides 35K+ live security attacks out of the box, with new attacks made available weekly, and the industry's only full coverage for Microsoft security updates within 24 hours of announcement
- Enables sophisticated attack simulation with more than 100 evasions, botnet-driven DDoS attacks, and more
- Simulates millions of users and blended application traffic at live network speeds of up to 40 Gigabits per second from a single three-slot chassis
- Scales to unlimited performance levels with multiple chassis managed via a single interface and configuration, with integrated reporting

Score Network, Data Center, and Device Resiliency with Standardized Scientific Measurements

- The BreakingPoint Storm produces the BreakingPoint Resiliency Score™, a deterministic, scientific, and repeatable measurement of network resiliency.
- Features the BreakingPoint Resiliency Score Lab, a wizard-like interface for standardizing measurement of devices and networks with virtually no configuration effort
- Enables customers to maintain ongoing resiliency by scoring and remediating issues as resiliency trends lower over time

Lower Total Cost of Ownership

- The BreakingPoint Storm is architected to adapt rapidly to change and ensure ongoing resiliency with the latest applications, security attacks, product features, and performance upgrades.
- All-inclusive pricing includes access to all applications and security attacks required for real-world simulations
- Backed by a dedicated group of security researchers and application protocol engineers committed to keeping the product completely current with frequent strike and protocol updates
- Easy to use by staff at all skill levels, from IT and security researchers to experts and technical marketing professionals
- Automated point-and-click capabilities and a library of prebuilt profiles reduce configuration time
- Scales easily to replace costly server farms or cyber range operations with a small, easy-to-maintain product