Spirent CyberFlood

Test the security, performance and scalability of your app-aware infrastructure
The Security and Application Challenge

The deployment of security application-infrastructure brings with it innovative capabilities for managing traffic, security and Quality-of-Service (QoS) policies. However, to accurately test application-aware infrastructures, it is critical to generate realistic packet payload that emulates actual application traffic on your network.

With many thousands of applications on the network and hundreds of new ones being released every day on millions of devices, QA, engineering and IT teams are struggling to quickly and effectively test, validate and roll-out their app-aware systems and networks.

The Solution: CyberFlood

CyberFlood is a powerful, easy-to-use test solution that generates realistic application traffic and attacks to test the performance, scalability and security of today’s application-aware network infrastructures.

Unlike other test solutions that use “fake” traffic with the same packet payload over and over again, CyberFlood provides 1G to >100 Gbps on a variety of platforms for stateful traffic testing with authentic, customizable payloads for realistic security, load, and functional testing.

In addition, CyberFlood keeps up to date with the latest Malware, DDoS and exploits to test the effectiveness of security operations.

Test and Enforce Application Policies
Verify the accuracy of application detection engines and policies by testing with thousands of popular application profiles.

Evaluate the impact of security policies on application performance with intermixed signature and DDoS attacks.

Recreate production-level mixes of application traffic and test the effectiveness of application QoS policies.

Benchmark Performance and Capacity
Benchmark scalability and network capacity by simulating thousands (or hundreds of thousands) of real users on the network.

Run “what-if” scenarios and measure the performance impact of architecture or configuration changes.

Validate proof-of-concept designs by testing with realistic mixes of application traffic.

Validate Network Security
Validate IPSec VPN capacities including tunnel setup, maximum tunnels and data rates over encrypted tunnel for remote access, and site to site use cases.

Verify the ability of security solutions to detect and mitigate thousands of known and zero day attacks.

Further challenge security solutions with encrypted attacks and easily add evasion techniques to create thousands of attack variations.

With CyberFlood fuzzing test the resiliency of network devices and deployed protocols by verifying the ability to deal with millions of unexpected and malicious inputs.

Test device capabilities to inspect traffic for malware, infected hosts, unwanted URLs and spam and take appropriate action.

NetSecOPEN tests Built-in
NetSecOPEN is a network security industry group where network security vendors, tool vendors, labs and enterprises collaborate to create open and transparent testing standards.
Test Next-Generation Security and Content-Aware Solutions

1. Get started quickly by choosing a pre-built test template.
2. Drag and drop traffic profiles into the player to easily customize tests.
3. Thousands of the latest apps and attacks are at your fingertips via the continually updated Spirent TestCloud.
4. Results are delivered in real-time in a customizable reporting interface.
5. Plus, test for Zero Day attacks with built-in fuzzing capabilities.
6. At-a-glance test grade reports showcase levels of Pass/Fail criteria for each new test run.

Spirent CyberFlood
Security
Find and fix vulnerabilities quickly
CyberFlood includes thousands of attacks, malware, and DDoS vectors, so you can test any mix of attacks and applications to ensure network security.
• Continually updated database of tens of thousands of attacks and malware samples
• Test any mix of attacks and applications
• Shorten resolution time with smart remediation tools
• Virtually unlimited test cases with Advanced Fuzzing
• Validate IPSec VPN capabilities, performance and capacities

Realism
Test your network, your traffic, your reality
CyberFlood includes the Spirent TestCloud™ for access to thousands of applications so you can generate traffic with authentic payloads for realistic security, load, and functional testing.
• Create tests with the latest apps from the Spirent TestCloud
• Capture and replay your network application traffic
• Create custom tests for unique apps and protocols
• Test advanced HTTPS and TLS traffic at load with high-strength ciphers and certificates
• Add hacker behavior to assessments with encrypted malware and attacks, and the use of evasions techniques to further stress security policies

Performance*
Extreme scale performance
CyberFlood is the world’s highest performing connection rate tester for HTTP, with more than 2x the current industry standard, giving you the power to push devices and networks to their limits.
• Stateful traffic generation from 1G to >100 Gbps rates
• >8.5M HTTP connections/second — the highest in the industry
• Realistic application packet payloads
• Over 170 million sustained connections per appliance

Agility
Test now, not months from now
The intuitive web-based CyberFlood UI makes it easy to design tests no matter what your experience level, so you can accelerate testing and complete projects more efficiently.
• Get started quickly with easy-to-use test methodologies
• Customize tests easily with the intuitive, browser-based UI
• Cloud-based content delivery
• Made for teams: share projects, tests, and results
• Cyber Range capabilities

* Performance only reflects C100-S3 capabilities, other platform options are available

Americas 1-800-SPIRENT
+1-800-774-7368 | sales@spirent.com
Europe and the Middle East
+44 (0) 1293 767979 | emeainfo@spirent.com
Asia and the Pacific
+86-10-8518-2539 | salesasia@spirent.com

© 2020 Spirent Communications, Inc. All of the company names and/or brand names and/or product names and/or logos referred to in this document, in particular the name “Spirent” and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice.