Data Sheet

spirent™
Promise. Assured.

Spirent **CyberFlood**

Applications and Security Test Solutions

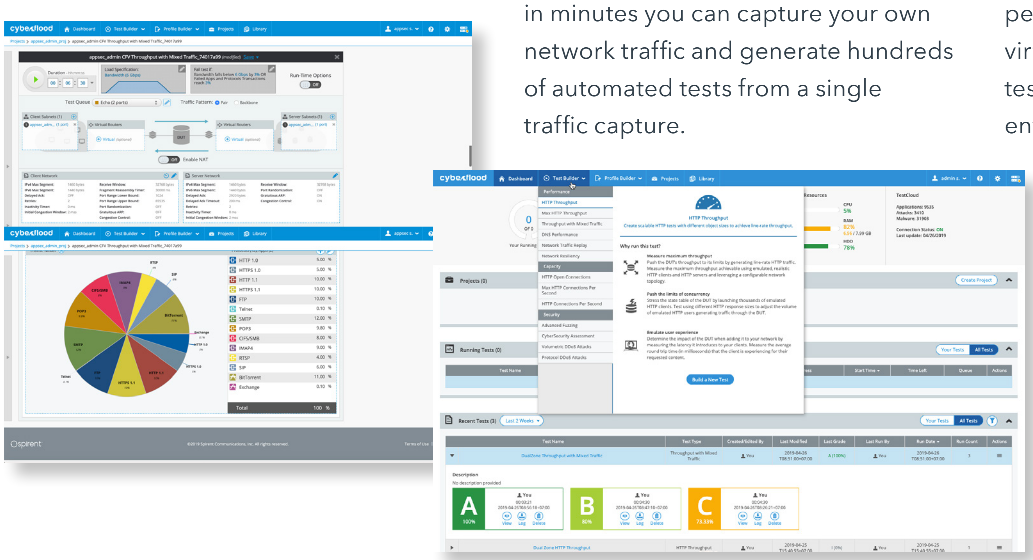
CyberFlood is a powerful, easy-to-use test solution that generates thousands of different realistic application traffic scenarios and attacks to test the performance, scalability and security of today's application-aware network infrastructures. Unlike other test solutions, CyberFlood generates real high-performance user applications based on actual application scenarios for realistic security, load and functional testing.

Applications

CyberFlood provides product development teams creating next generation content-aware devices and solutions a competitive advantage by helping them get to market more quickly with proven scalability, security and performance. Enterprise and Lab Engineers can ensure the solutions they deploy will deliver the security required.

With CyberFlood, users can quickly and easily test with the latest and greatest applications and attacks (updated continuously), all with unparalleled realism and scalability. Users can push their solutions to the limit while ensuring the infrastructure will stand up to real-world demands.

- **Realism—test your network, your traffic, your reality:** When testing application-aware devices, it is critical that the application mix reflects real-world conditions from Layer L2-7. CyberFlood enables you to create tests by capturing the interactions of real users, on real devices, as they use real applications on your network for unprecedented realism for testing.
- **Agility—test now, not months from now:** CyberFlood includes our TestCloud, giving you access to thousands of ready-to-run performance and security tests and the ability to create new tests as soon as new applications or protocols emerge. With thousands of user scenarios—from mobile handset-based applications to the latest in P2P file transfer—CyberFlood delivers. Plus, in minutes you can capture your own network traffic and generate hundreds of automated tests from a single traffic capture.
- **Security—find and fix vulnerabilities quickly:** Spirent TestCloud includes thousands of known attack profiles, so you can test any mix of attacks and applications to verify and analyze network security. For malware-testing we provide infected host emulation, and malware binary transfer-based security testing. Plus, you can quickly create custom tests for unique protocols and applications without scripting, and leverage smart remediation tools to shorten the time to fix vulnerabilities.
- **Flexibility—The right solution for your needs:** CyberFlood is available on a number of diverse platforms to meet your specific needs. Portable solutions for on-the-go testing, appliances that support 1G, 10G, 25G, 40G, 50G and 100G native speeds for higher performance and capacities, and fully virtualized solutions for unbounded testing of SDN/NFV devices and environments.



Features & Benefits

- **Throughput with Mixed Traffic:** Create and run tests with preconfigured traffic mixes to achieve high throughput SSL/TLS encryption, or create your own mixes from a database of thousands of application scenarios and blend in attack traffic to verify security policies under load.
- **Cybersecurity Assessment:** Run tens of thousands of modern and advanced attacks, DDoS and malware (both binary transfer and infected host emulation).
- **Application Identification:** Create high volumes of the latest mobile and cloud apps, and security traffic patterns with 1000's of apps from TestCloud. Our libraries are updated continually, downloaded directly, ensuring you have the most popular and relevant apps and attacks for your testing needs.
- **High-Scale Throughput:** Create tests that operate from 1Gbps to 100Gbps rate to push the bounds of carrier class devices and network services.
- **Projects:** Create groups of tests with common objectives to be worked on by multiple team members, greatly improving test lab efficiencies.
- **Traffic Replay:** Replay and scale captured traffic recreating conditions from your own environment. Replay large files "as is" to maintain the original traffic fidelity, or modify the amount of traffic. Also, overwrite IP and MAC addressing on the captured traffic to test under new conditions.
- **High-Scale Connections per Second:** Quickly create tests to verify encrypted and/or non-encrypted capacity a device or network can handle.
- **SmartMutation™ based-fuzzing:** Perform different service and protocol mutation scenarios (including server response fuzzing) to find vulnerabilities and test the reliability of implemented protocols with millions of test iterations created on-the-fly. Define what protocol component to test. Repeat exact fuzz iteration for reproduction of the fault event.
- **Reliability Testing:** Perform long duration soak tests with the TestCloud application load to ensure solutions work at high capacity for long periods of time.
- **NetSecOPEN:** NetSecOPEN is a network security industry group where network security vendors, tool vendors, labs and enterprises collaborate to create open and transparent testing standards.
- **Global IP Selector:** Quickly select where emulated traffic is created by selecting global regions on a map.

Platform Options

- **C1 Portable Appliance**
  4 x 1G, 2 x 10G and 4 x 1G and 2 x 10G options
- **CF20 1U Self Contained Appliance**
  4 x 1G, 8 x 1G, 8x10G, 2 x 40G, and 2 x 100G interface options
- **C100-S3 Ultra Performance Appliance**
  16 x 1G, 8 x 10G, 16 x 10G, 4 x 25G, 4 x 40G, 4 x 50G, 4 x 100G options
- **CyberFlood Virtual**
  ESXi or KVM instances—flexible scalability
- **AWS and Azure**
  Deployments for use in cloud environments

System Requirements

Client—The client used to access the virtual host must meet the following minimum requirements to run the CyberFlood: Any Windows, Mac or Linux PC running the latest browsers versions (June 2017 or greater); Firefox browser, Google Chrome browser

Virtual Host—User provided virtual host systems must meet the following minimum requirements to run the CyberFlood Virtual Host software

- VMware vSphere Hypervisor ESXi—(v5.1.0 or higher, 64-bit only, bare metal)
- KVM on Linux—(64-bit only, bare metal)
- 128G Hard Drive
- 8G RAM
- 2+ GHz Dual Core Processor (64-bit)
- VT extensions enabled for 64-Bit OS
- Dedicated network interface with a static IP address

Ordering Information

Description	Part Number
CyberFlood Base License for C100	CF-SW-BASE
CyberFlood Cyber Security Suite	CF-SW-CYBER
CyberFlood Volumetric DDoS Suite	CF-SW-DDOS
CyberFlood Dns Test Methodology	CF-SW-DNS
CyberFlood Emix Tests—Throughput with Mixed Apps	CF-SW-EMIX
CyberFlood HTTP Open Conns Testing Methodology	CF-SW-HCONNS
CyberFlood Max HTTP Throughput Testing Methodology	CF-SW-HMAX
CyberFlood Protocol DDoS	CF-SW-PDDOS
CyberFlood Traffic Replay	CF-SW-TRAFFREP
CyberFlood Advanced Malware Content-1Yr	CF-C-ADVMALWARE-1Y
CyberFlood Attacks Content-1Yr	CF-C-ATTACKS-1Y
CyberFlood Standard Malware Content-1Yr	CF-C-MALWARE-1Y
CyberFlood TestCloud Apps Content-1Yr	CF-C-TESTCLOUD-1Y
CyberFlood CyberSiege Global IP Traffic Selector-1Yr	CF-SW-IANA-1YR

Other CyberFlood options are available for specific hardware platforms and Advanced Fuzzing options, please contact Spirent sales for more information.

Contact Us

For more information, call your Spirent sales representative or visit us on the web at www.spirent.com/ContactSpirent.

www.spirent.com

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