

# CyberFlood

Simple, accurate testing and validation for modern, app-centric networking devices and solutions

## Get a reality check on performance, scalability, and security

Modern app- and content-aware infrastructures promise innumerable benefits. Network architectures such as SD-WAN, SASE, and others can dramatically accelerate performance, network availability, and security while simplifying the management of policies across the entire landscape.

All of these capabilities can give your business the ability to seamlessly scale on demand, protect devices at the edge, and more — **if you have accurate, reliable testing and validation.**

However, traditional testing methods continue to fall short. DevOps, QA, and IT teams still struggle to keep pace with testing as the sheer volume of applications and infrastructure permutations continues to grow on an upward spiral.

CyberFlood provides a stunningly simple and effective solution.

CyberFlood lets users quickly test and validate performance and scalability on any modern app-ware devices and solutions. CyberFlood lets you stress-test your network devices using the latest applications (updated continuously) and push performance and scalability to the limit—so you can see what's working and what could be improved. With the optionally licensed security testing solution, you can also validate security efficacy of today's modern security devices and counter measures.

## Use real traffic for realistic, accurate results

### Test and Enforce Application Policies

- Verify the accuracy of application detection engines and policies by testing with tens of thousands of popular application scenarios, as well as next generation web protocols, such as HTTP/3.
- Evaluate the impact of security policies on application performance and availability.
- Recreate production-level mixes of application traffic and test the effectiveness of network 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, security, and configuration changes.
- Validate proof-of-concept designs by testing with realistic mixes of application traffic.

### NetSecOPEN Tests Built In

Leverage the combined innovations and expertise of network security vendors, tool vendors, labs, and enterprises that have collaborated to create open and transparent testing standards for modern contentaware solutions

## Key Features and Capabilities

- **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 tens of thousands of application scenarios to verify performance under load.
- **Application Identification:** Create high volumes of the latest mobile and cloud applications with tens of thousands of apps from TestCloud. The TestCloud libraries are updated continually and downloaded directly, ensuring you have the most popular and relevant apps for your testing needs.
- **Advanced Mixed Traffic Assessment:** Create custom and highly configurable tests and assessments with user action lists that execute a set of user application interactions for HTTP, HTTP/2, HTTP/3, HTTPS, SMTP, POP3, IMAP4, FTP, DNS over TLS and HTTPS, and other protocols.
- **High-Scale Throughput:** Create tests that operate from 1Gbps to terabit scale to push the boundaries of carrier class devices and network services
- **Automatic Goal Seeking:** Determine maximum capabilities of a device with minimal user interaction.
- **VPN Assessment:** Validate IPSec and SSL VPN capacities including tunnel setup, maximum tunnels, and data rates over encrypted tunnels for remote access and site-to-site use cases.
- **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.
- **High-Scale Connections per Second:** Quickly create tests to verify encrypted and/or non-encrypted capacity that a device or network can handle.
- **Reliability Testing:** Perform long duration soak tests with the TestCloud application load to ensure solutions work at high capacity for long periods of time.
- **Global IP Selector:** Quickly select where emulated traffic is created by selecting global regions on a map.
- **Automation:** Use the RESTful API to fully automate the CyberFlood UI, allowing vast regression test beds to be set up for ongoing use cases.

## Available on Multiple Platforms

- **C1 Appliance** — Portable bench level testing (10G/1G)
- **Cf30 Appliance** — Selfcontained, portable 1G and 10G interface testing
- **C100-S3 Appliance** — High end performance and capacity for a wide range of applications
- **C200 Appliance** — For carrier class assessments and unparalleled cryptographic validation capacities
- **C200 Appliance** — For carrier class assessments and unparalleled cryptographic validation capacities

## The CyberFlood advantage

### Performance at extreme scale

CyberFlood is the world's highest performing connection rate tester for HTTP, with more than 2 times the current industry standard, giving you the power to push devices and networks to their limits. Available in a multitude of platforms capable of:

- Stateful traffic generation from 1G to >400 Gbps rates
- >4.0M HTTP connections/second — the highest in the industry
- Hyper-realistic application emulation
- Over 170 million sustained connections per appliance
- Auto performance goal-seeking tests

### Extreme agility

Test now, not months from now. The intuitive webbased CyberFlood UI makes it easy to design tests no matter what your experience level, so you can accelerate testing and complete projects more efficiently.

- Test every deployment environment: SDWAN, SASE, IPSec, and more—from basic traffic to multiple 100G speeds
- Get started quickly with easy-to-use test methodologies
- Customize tests easily with the intuitive, browser-based UI
- Share projects, tests, and results in teamoriented environments to maximize use and your investment

### Extreme realism

Test your network, your traffic, and your reality. CyberFlood includes Spirent TestCloud for access to tens of 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 to model tests based on your reality
- Create custom tests for unique apps and protocols
- Test against targeted systems and applications acting as high scale users
- Test advanced HTTPS and TLS traffic at load and scale with high-strength ciphers and certificates
- Use web-capture capabilities to import and replay recorded sessions of complex website interactions and traffic to validate performance and comprehensive application

### Objective, vendorneutral testing

When you test and validate with CyberFlood, you're harnessing a testing solution that conforms to all relevant industry standards and specifications, including:

- MEF
- Standards from all segments of the network communications market
  - High-speed Ethernet
  - IPSec
  - SD-WAN
  - SASE and Zero-Trust

## Optional Advanced Security Testing Capabilities

With Spirent CyberFlood security testing (licensed separately), you can:

- Test your security devices and solutions using tens of thousands of up-to-date application, attack, and malware scenarios to verify and analyze network security.
- Add realistic hacker behavior with evasion techniques or encrypt attacks to push security solutions to further stress their limits.
- Quickly create custom tests for unique protocols, traffic flows, and applications without scripting.
- Challenge security solutions with encrypted attacks and easily add evasion techniques to create thousands of attack variations.
- Utilize the MITRE ATT&CK™ framework to align security testing with production vulnerability, modeling industry techniques.
- Leverage smart remediation tools to shorten the time to fix vulnerabilities.
- Verify the ability of security solutions to detect and mitigate thousands of known and zero-day attacks.



📍 203, Ansal Chamber-II, 6, Bhikaji Cama Place, New Delhi-110066  
📞 +91 11 26700500/26103358 📠 +91 11 26183229 📧 +91-9212605204  
🌐 marketing@savitritelecom.com

@2022 Savitri Telecom Services  
Product specifications and descriptions in this document are subject to change without notice.  
@1222STSACds-CF-001