CyberFlood

Application Performance Testing Solution

CyberFlood is a powerful, easy-to-use test solution that generates tens of thousands of realistic application traffic scenarios to test the performance and scalability of today's application-aware network infrastructures. Available as both high-performance appliances and a fully virtualized solution, CyberFlood enables organizations to test physical, virtual, and cloud environments with unmatched realism and scale.

The deployment of modern application-centric infrastructures introduces innovative capabilities for managing traffic, Quality-of-Service (QoS), and security policies. To accurately validate these environments, it is critical to generate realistic user activity that emulates actual application traffic behavior on the network.

With CyberFlood, users can quickly and easily test with the latest and greatest applications (updated continuously) 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, the application mix must reflect real-world conditions. CyberFlood enables users to create tests by emulating the interactions of real users on real devices using real applications.

Using built-in web-capture capabilities, users can import and replay recorded sessions of complex website interactions and traffic to validate performance and comprehensive application policies.

Ease of Use — VIAVI Model Context Protocol (MCP) Server Framework: An AI-native natural language integration for network and security test workflows. The CyberFlood MCP server exposes product-specific standardized tools and resources for external AI agents, enabling custom agentic workflows via natural-language-driven test execution, results analysis and test automation.

Applications

CyberFlood supports a wide range of validation use cases across enterprise, service provider, and lab environments. It enables teams to verify application performance, scalability, and policy enforcement before deployment.

Applications include:

- Testing next-generation firewalls and security devices
- Validating SASE, SD-WAN, and cloud environments
- Generating application traffic to verify QoS and QoE policies
- Performing AI/LLM inference and application validation
- Replaying captured production traffic at scale

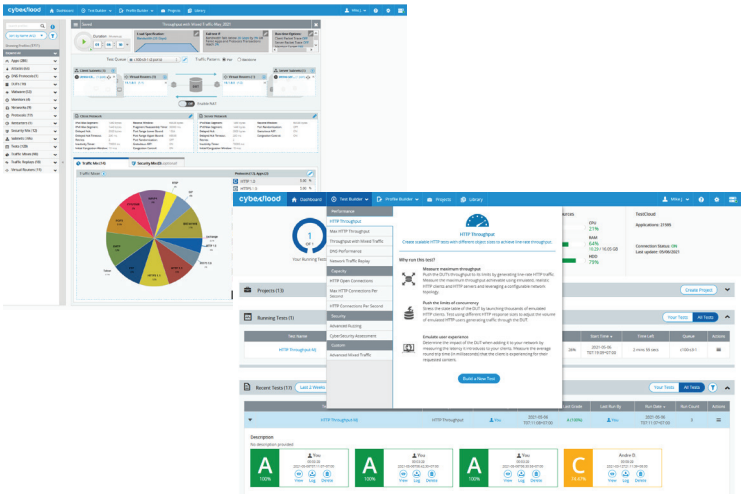
Optional advanced security testing solutions are also available for CyberFlood.

Agility — test now: CyberFlood TestCloud provides tens of thousands of ready-to-run application scenarios, ranging from mobile applications to streaming, social, and AI-driven traffic.

Users can quickly generate new tests as applications and protocols evolve. In addition, traffic capture capabilities allow multiple automated test scenarios to be created from a single capture, reducing setup time and enabling rapid validation cycles.

Flexibility — The right solution for your needs: CyberFlood is available on a number of diverse platforms to meet different testing requirements. Physical appliances deliver deterministic, high-performance testing, while CyberFlood Virtual provides a flexible, software-based approach for cloud and virtualized environments.

CyberFlood Virtual can be deployed on VMware ESXi, KVM, and cloud platforms including AWS, Azure, and Google Cloud, enabling testing of SDN/NFV, SASE, and cloud-native architectures with scalable compute resources.



Features and Benefits

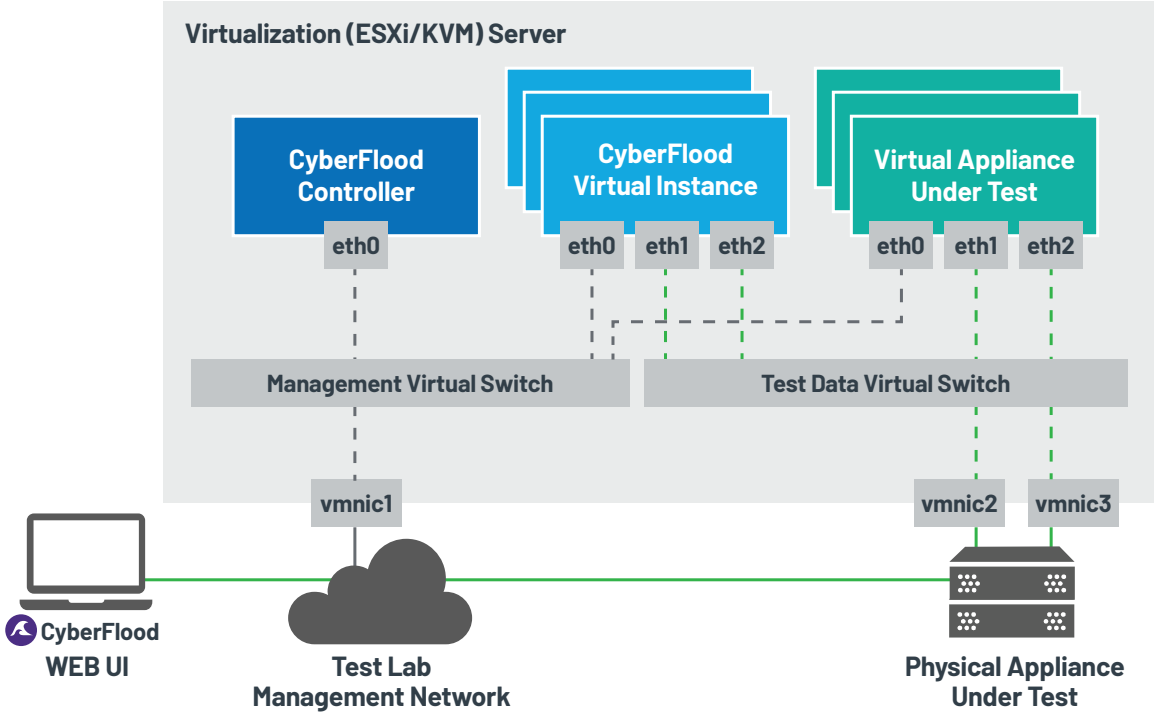
- **Throughput with Mixed Traffic:** Create and run tests with preconfigured traffic mixes to achieve high throughput SSL/TLS encryption, or create your own mixes from a database of hundreds of thousands of application scenarios to verify performance under load.
- **VIAVI MCP Server Framework, Part of the VIAVI NITRO® AI portfolio:** enables users to configure, execute, and analyze complex test scenarios through a natural language AI interface, eliminating time-consuming GUI-based workflows and minimizing the need for deep product training.
- **Test the Future of Encryption:** CyberFlood is the first testing platform to bring quantum-safe cryptography to performance testing. With support for NIST's FIPS 203/204 PQC cipher suites PQC cipher suites and hybrid KEMs such as X25519Kyber768, CyberFlood validates readiness, identifies compatibility risks, and helps you plan for next-gen security upgrades—without compromising performance or QoE.
- **Application Identification:** Create high volumes of the latest mobile and cloud applications with hundreds 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. Create tests that use next generation web protocols, including the industry's first support for HTTP/3.

- **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.
- **AI/LLM Policy and Security Validation:** CyberFlood tests 36 GenAI apps with editable prompts to detect LLM threats such as prompt injection and measures policy impact on performance and QoE.
- **High-Scale Throughput:** Create tests that operate from a 1Gbps to 100Gbps rate to push the bounds of carrier class devices and network services.
- **IPSec Assessment:** Create comprehensive assessments of IPSec VPN setup rates, concurrent tunnels, and data rates.
- **Automatic Goal Seeking:** Determine maximum capabilities of a device with minimal user interaction.
- **SSL VPN:** Test tunnel setup and data traffic throughput capacity over an expanding set of SSL VPN dialects. Create comprehensive scale and accuracy tests with full control over data plane traffic profiles.
- **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.
- **NetSecOPEN Built-in Tests:** NetSecOPEN is a networking industry group where networking vendors, tool vendors, labs and enterprises collaborate to create open and transparent performance testing standards for today's modern content-aware solutions.
- **ZTNA Testing:** Test the Zero Trust Policy Enforcement Point (PEP), validate that secure network and application access are delivered and verify that connections and per-user access policies are functioning as intended without impacting performance or QoE.
- **Container Support Cloud-Native Platforms:** Open-source Kubernetes, OpenShift, AWS EKS, and VMware TKG

Platform Options

- **CF50 1U Self-Contained Appliance**
  8 x 1G/10G, 2 x 100G
- **CF400 High-Density Carrier Class Performance Appliance**
  16 x 10G, 16 x 25G, 8 x 40G, 8 x 50G, 8 x 100G
- **CyberFlood Virtual**
  - VMWare ESXi
  - KVM on Linux
  - Proxmox
  - OpenStack
- **Amazon AWS, Azure, and Google Cloud (GCP)**
  Deployments for use in cloud environments

CyberFlood Virtual Logical Topology



2143.900.1225

System Requirements

Client — The client used to access the virtual host must meet the following minimum requirements to run CyberFlood: Any Windows, Mac or Linux PC running the latest versions of 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 (v6.50 or higher, 64-bit only, bare metal)
- KVM on Linux (64-bit only, bare metal)
- 320G Hard Drive
- 16G RAM
- 2+ GHz Dual Core Processor (64-bit)
- VT extensions enabled for 64-Bit OS
- Dedicated network interface with a static IP address

Virtual Cores and Traffic Generation — License the number of CPU cores to size CyberFlood to meet your specific scale and performance needs. Minimum requirements:

- 2 Ghz or greater CPUs
- 4 x vCPUs per virtual instance
- 8G RAM per virtual instance

VIAVI Services

Education Services Instructor-led training: Hands-on methodology and product training .

Ordering Information

Part Number	Description
CF50	
CF-KIT-001-CF50	CF50 Base Appliance Kit 8x10G/1G SFP+ and 2x100G QSFP28 add-on for existing CF Controllers
CF-KIT-002-CF50	CF50 Performance Kit 8X10G/1G SFP+ and 2x100G QSFP28
CF400	
CF-KIT-001-CF400	CF400 Base Appliance Kit 8 x QSFP28 (add-on unit)
CF-KIT-002-CF400	CF400 Performance Kit 8 x QSFP28
CF-KIT-004-CF400Q	CF400 Multi-speed Base Appliance Kit 8 x QSFP28 (add-on unit)
CF-KIT-005-CF400Q	CF400 Multi-speed Performance Kit 8 x QSFP28
CyberFlood Virtual	
CFV-PERF-SUB	Includes: DNS Test Methodology, Throughput With Mixed Apps (Default Protocols), HTTP Open Conns Testing Methodology, Traffic Replay
CFV-VCORES-04-SUB	CyberFlood Virtual Instance 4 Cores, yearly subscription
CFV-VCORES-08-SUB	CyberFlood Virtual Instance 8 Cores, yearly subscription
CFV-VCORES-16-SUB	CyberFlood Virtual Instance 16 Cores, yearly subscription
CFV-VCORES-32-SUB	CyberFlood Virtual Instance 32 Cores, yearly subscription

CyberFlood is available on a variety of Hardware, Virtual, Cloud, and Container platforms with software bundles to meet your specific needs and use cases. Advanced Security Testing options are also available.

CyberFlood Appliance Performance Kits include: HTTP Throughput, HTTP CPS, HTTP Concurrent Connections with TLS/PQC, DNS, Throughput with Mixed Traffic (default protocols), Advanced Mixed Traffic, and Network Traffic Replay test methodologies.

CyberFlood Virtual is also available in perpetual licensing options, functional performance licensing, and multi-year license options.

Contact VIAVI Sales for more information on CyberFlood solution offerings.

Contact Us: +1 844 GO VIAVI | (+1 844 468 4284). To reach the VIAVI office nearest you, visit viavisolutions.com/contact

© 2026 VIAVI Solutions Inc. Product specifications and descriptions in this document are subject to change without notice. Patented as described at viavisolutions.com/patents

cyberflood-appperf-ds-hse-nse-ae
30194791 903 0826