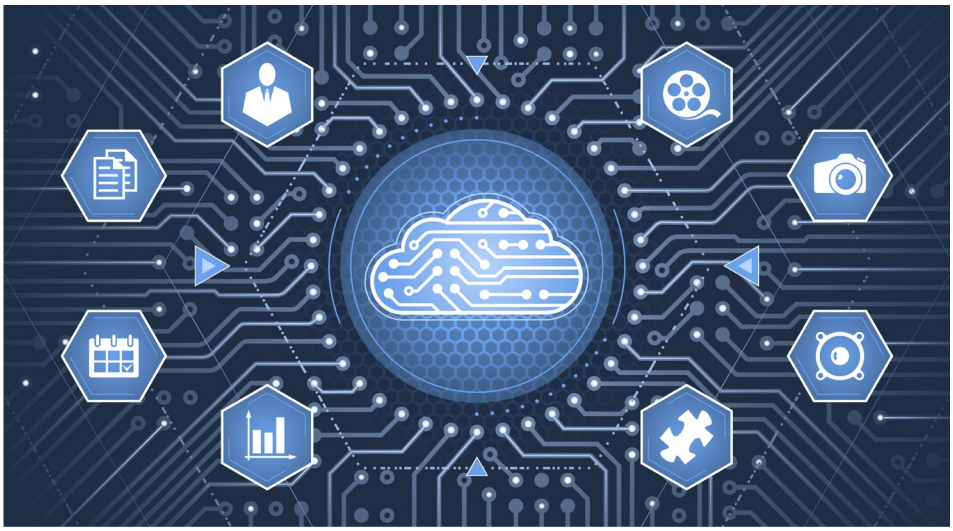
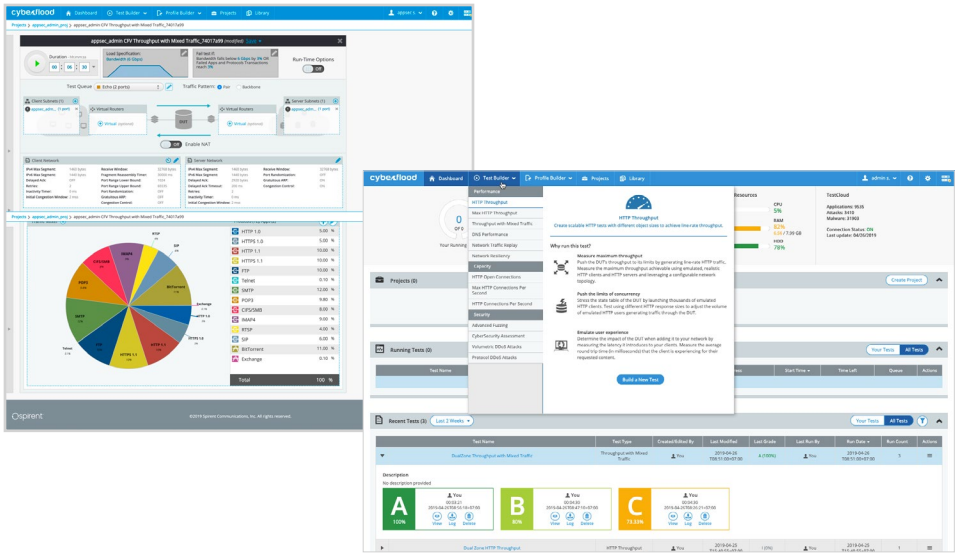
DATASHEET

Spirent CyberFlood Virtual

Applications and Security Test Solutions



Software Defined Networking reduces infrastructure cost and overhead by opening a new world of flexibility, scale and performance for enterprises. The convergence of network and application infrastructures into a single extensible and flexible platform requires improved levels of understanding of network security effectiveness and performance. Spirent CyberFlood Virtual is a flexible solution that offers proactive and realistic testing of content aware networks and security infrastructure that is easily hosted on users premises or compatible cloud based infrastructures.



Spirent's revolutionary CyberFlood security and application testing solution is now available as a virtual platform offering you simplified use, by consolidating multiple test functions into a completely virtual test environment.

CyberFlood virtual offers validation of security posture, Quality of Service (QoS) and Quality of Experience (QoE) through quick and simple to use tests of cybersecurity assessment and performance of network infrastructures.

Applications

- Test SDN environments directly from within a virtual environment with multiple unbounded traffic generation endpoints
- Scale test solutions to handle vast amounts of traffic based on your needs
- Verify NFV security effectiveness with real attacks and exploits
- Test DDoS mitigation services and Next Generation Firewalls
- Generate application load traffic from a growing database of over 15,000 user scenarios and application flows to verify application ID policies and performance
- Advanced mixed traffic assessment allows you to create custom user actions including IPSec VPN capacity and throughput tests
- Validate performance and security with Amazon Web Service (AWS) environments, Azure, and Google Cloud (GCP)
- Test with zero-day and up-to date malware scenarios
- Replay custom traffic at scale
- Assess SD-WAN environments for scale, performance and security efficacy
- Functional performance licensing available for lower cost and higher virtual instance density use cases

User Realism with CyberFlood

CyberFlood utilizes TestCloud™ for access to thousands of applications so you can generate traffic with authentic payloads for realistic security, performance load and functional testing. CyberFlood creates tests with the latest apps from the Spirent TestCloud, while also providing the ability for users to import their own applications to recreate custom application at scale.

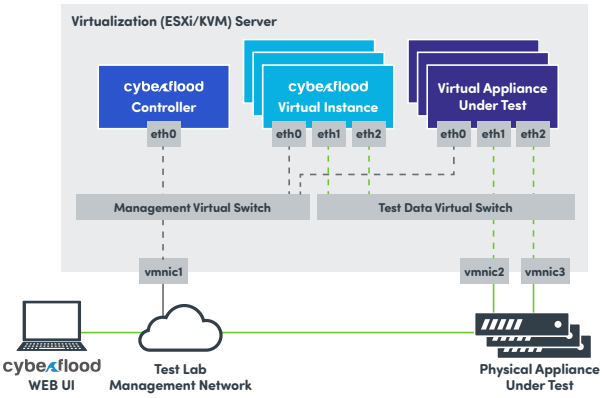
Quickly test with recent attacks and their variants like Wannacry, Petya, Crisis, Nemucod, Spora, Cerber and more. CyberFlood provides access to an always up-to-date database of thousands of attacks, real malware profiles and vectors, so you can test any mix of attacks and applications at scale. Quickly and easily determine how security polices work to defend against attacks while allowing legitimate user traffic to pass through as unimpeded as possible. Test with high scale volumetric and protocol DDoS to verify mitigation policies are up to task.

Features & Benefits

- **Ease of Use—**Extremely easy to use and highly intuitive graphical user-interface that allows for difficult configurations to be set up instantly; from setting up global IPs from a world view map to drag and drop protocols, CyberFlood makes security and performance testing easy.
- **Economical—**CyberFlood Virtual comes in a number of license simple annual subscription options to meet your use case and performance needs. From basic performance testing to a full suite of security testing with updated content you can choose the right solutions for your needs.
- **Cloud Assessment—**CyberFlood Virtual can be installed on specific cloud infrastructures, such as AWS, Azure, and Google Cloud (GCP) to validate and verify performance of default an/or third party cloud based security or traffic inspection solutions.
- **Flexible—**Change the system resources of vCores and memory assigned to CyberFlood Virtual traffic generators to build systems that meet your specific needs.
- **Network Security Testing—**Provides extensive testing for secure network communication, vulnerability assessment with an ever growing and up-to-date database of over 4,000 exploit profiles and over 50,000 malware samples.
  - Add hacker behavior to assessments from a series of evasions techniques that create attack and malware variations on-the-fly to further challenge security counter measures.
  - Verify the ability of the network security devices to detect and mitigate thousands of known and zero day attacks.
  - Send TCP based attacks and malware over TLS to validate detection of attacks that are hidden by encrypted traffic flows.
  - 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 for common web protocols.
  - Test network device capabilities to inspect traffic for malware, infected hosts, unwanted URLs and spam and take appropriate action.
  - Validate IPSec VPN capacities including tunnel setup, maximum tunnels, and data rates over encrypted tunnel for remote access, and site to site use cases.
- **Applications—**With CyberFlood, users can quickly and easily test with the latest and most popular 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.
- **Advanced HTTPS Testing—**CyberFlood Virtual provides extensive coverage to test and stress HTTPs traffic at scale. Highly configurable with cipher type, cert size and a variety of other parameters allows users to make highly realistic HTTPS and mixed traffic tests quickly and easily.
- **CyberFlood Virtual** can also be used with the Avalanche application testing solution
- **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.

Technical Specifications	
Virtual Environments	
Virtual Instances	VMWARE ESXi 5.5, 6.0, 6.5 KVM on Linux (64-bit only, bare metal) AWS Azure Google Cloud (GCP)
Virtual Cores	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 • 60GB HDD provisioning • AWS instance types supported - c5.9xlarge, c5.xlarge, m4.xlarge
Virtual Controller	VMWARE ESXi 5.1 to 6.5 KVM on Linux (64-bit only, bare metal) • 2 x vCPUs • CyberFlood Controller to be used for AWS
Licensing	
CyberFlood Performance Testing license	Comes with HTTP/HTTPS bandwidth, connectivity and rate testing, advanced mixed traffic testing, custom traffic replay and DNS
CyberFlood Security and Performance Testing Software license	Comes with All CyberFlood options covering CyberSecurity Assessment for malware and attacks, DDoS testing and all performance testing software options
CyberFlood TestCloud subscription	Allows options for always up-to-date download-able content for application scenarios, attacks/ exploits and malware
Avalanche Support	CyberFlood Virtual instances support Avalanche for deep session web testing
CyberFlood Features	
Advanced Fuzzing	CyberFlood provides powerful options for fuzz testing over common web protocols
Web Based Interface	Easy to use multi-user web-based interface makes setting up and executing comprehensive tests fast, easy and consistent
Application Scenarios	Over 15,000 current and popular application and user scenarios
Attack and Exploits	Over 4,000 attacks and exploits covering areas such as SQL injection, cross site scripting, targeted OS, in-line device, endpoint services and more
Malware	Over 50,000 recent and zero-day malware samples including command and control behavior and binary, malware transfer scenarios
DDoS	Test security mitigation policies by using different DDoS attacks to confirm its ability to detect and block them successfully with a suite of volumetric and protocol DDoS attacks that can be configured for stand-alone attack tests or mixed with normal user traffic to verify impact on performance
HTTPS/TLS Testing	Support for SSLv3, TLS v1.0, TLS v1.2, and TLS v1.3 with selectable certificate and cipher suites
Advanced Mixed Traffic Assessment	Create custom and highly configurable tests and assessments with user action lists that allow test assessments to be created which will walk through a set of user application interactions for HTTP, HTTPS, SMTP, POP3, IMAP, and FTP protocols (additional protocol support coming soon)
CyberSecurity Assessment	Quickly create tests that verify the effectiveness of IDS, IPS NGFW and other security solutions with and without user load of traffic
HTTP/HTTPS Connections Tests	Open thousands to millions of new connections per second to ensure your DUT can handle the new connection rate of your network
HTTP/HTTPS Bandwidth Tests	Find the maximum throughput achievable using emulated, realistic HTTP clients and HTTP servers and leveraging a configurable network topology
HTTP/HTTPS Open Connection Tests	Open millions of concurrent TCP connections within the state table of your DUT to find the maximum concurrency it can support. Leverage HTTP as the protocol for added realism during this test
VPN Testing	Easily assess capacities and capabilities of site to site and remote access IPSec from tunnel setup to data traffic handling
Mixed Traffic Tests	Measure the impact on application performance when using real-world built-in applications or extended with the power of TestCloud. Individually measure the bandwidth and success rate of each application added to the test to confirm the impact of the network under test
Traffic Replay	Replay your own traffic profiles at scale to determine the impact of customer traffic flows on network devices and services
DNS Tests	Overload your DUT by sending hundreds of thousands of DNS queries per second for it to process and traverse through it as well as for it to process the corresponding events that occur on the DNS responses

Logical Topology



Requirements

The web browser minimum requirements to access CyberFlood controller are:

- Google Chrome (v34.0.1847.131)
- Firefox web browser (version 29.0)
- And minimum screen resolution is 1280 x 800

Spirent Services

Professional Services

- Test lab optimization: Test automation engineering services
- Service deployment and service-level optimization: Vendor acceptance testing, SLA benchmarking, infrastructure and security validation
- Device scalability optimization: POC high scalability validation testing

Education Services

- Web-based training: 24x7 hardware and software training
- Instructor-led training: Hands-on methodology and product training
- Certifications: SCPA and SCPE certifications

Implementation Services

- Optimized new customer productivity with up to three days of on-site assistance

Ordering Information

Description	Part Number
CyberFlood Virtual Performance License 1 Year Includes: DNS Test Methodology, Throughput With Mixed Apps (Default Protocols), HTTP Open Conns Testing Methodology, Traffic Replay	CFV-PERF-1Y
CyberFlood Virtual Security Performance License 1 Year Includes: DNS Test Methodology, Throughput With Mixed Apps (Default Protocols), HTTP Open Conns Testing Methodology, Traffic Replay,TestCloud, Attacks, Advanced Malware, Global IP , Cyber Security Suite, Volumetric DDoS*	CFV-SECPERF-1Y
CyberFlood Virtual Instance 4 Cores 1 Year	CFV-VCORES-04-1Y
CyberFlood Virtual Instance 8 Cores 1 Year	CFV-VCORES-08-1Y
CyberFlood Virtual Instance 16 Cores 1 Year	CFV-VCORES-16-1Y
CyberFlood Virtual Instance 32 Cores 1 Year	CFV-VCORES-32-1Y

CyberFlood Virtual is also available with functional performance licensing and multi-year options, please contact Spirent sales for more information

*DDoS not supported in CyberFlood Virtual Functional performance version.

About Spirent Communications
Spirent Communications (LSE: SPT) is a global leader with deep expertise and decades of experience in testing, assurance, analytics and security, serving developers, service providers, and enterprise networks. We help bring clarity to increasingly complex technological and business challenges. Spirent's customers have made a promise to their customers to deliver superior performance. Spirent assures that those promises are fulfilled. For more information visit: **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

Rev K | 10/20