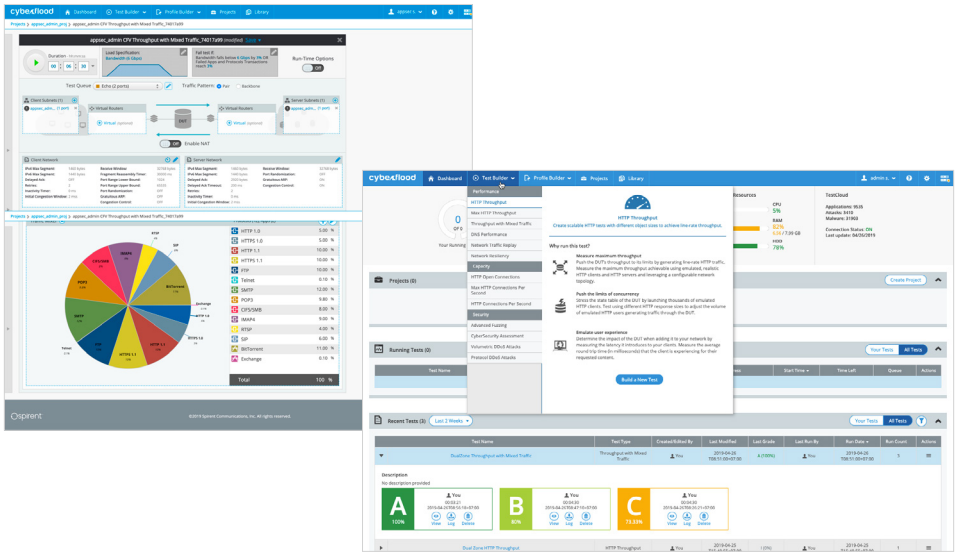
DATASHEET

Spirent CF20
for CyberFlood

Applications and Security Test Solutions

Understanding network security effectiveness and performance are crucial for today's demanding business environments, users today demand high-access and failsafe security Proactively testing content aware networks and security infrastructures is now more accessible than ever with the Spirent CF20 CyberFlood testing platform. Spirent's CF20 is sized right and feature rich to meet very demanding security and performance testing needs. It's multi-speed allows for a wide array of use cases and covers the majority of network interfaces in use today with options from 1G to 100G for use in enterprises, data centers and service providers. The CF20 is a fully self-contained solution with built-in web-based test controller to manage test cases and assets and comes standard with advanced crypto-acceleration to create vast amounts of high-depth HTTPS traffic at scale.



The CF20 for CyberFlood solution provides advanced test options for 1G, 10G, 40G and 100G interfaces. The CF20 tests the security effectiveness and performance of network infrastructures, web application infrastructure to verify your security posture, Quality of Service (QoS) and Quality of Experience (QoE). The CF20 uses the power of CyberFlood, offering you simplified use, by consolidating multiple test functions into a single small form factor appliance.

Applications

- Verify security effectiveness with real attacks and exploits
- Test DDoS mitigation services and Next Generation Firewall
- Create extreme loads of HTTPS traffic to verify encryption capacity and performance
- Generate application load traffic from a growing database of over 20,000 user scenarios and application flows to verify application ID policies and performance
- Test with zero-day and up-to date malware samples
- Replay custom traffic at scale
- Advanced mixed traffic assessment allows you to create customer user actions including IPSec VPN capacity and throughput tests

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 firewall 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. The CF20 also offers a reduction in deployment and management complexity due to easy out-of-box setup.
- **Economical—**Access the power of CyberFlood with the right features, performance and capabilities in a low profile package without comprising on performance. In addition, there is also a reduction in cost ownership due to lesser requirements for rackspace, power and cooling.
- **Network Security Testing—**Provides extensive testing for secure network communication, vulnerability assessment with an evergrowing and up-to-date database over 4,000 exploit profiles and over 70,000 malware samples.
  - Verify the ability of the network device to detect and mitigate thousands of known and zero day attacks.
  - 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.
  - 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.
  - Send TCP based attacks and malware over TLS to validate detection of attacks that are hidden by encrypted traffic flows.
  - Test 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.
- **Power and Performance—**The right performance and scale: The CF20 provides the right performance profile to effectively exercise networks to find maximum user connectivity, application traffic throughput capabilities, and security effectiveness. With up to 60Gbps of HTTP traffic generation capabilities.
- **Built-in Cryptographic Acceleration—**The CF20 comes with standard built-in cryptographic acceleration technology to increase the scale of encrypted traffic rates and bandwidth, including strong and current cipher types.
- **Cross Compatibility—**The CF20 offers test compatibility with other CyberFlood platforms, this provide maximum flexibility for using CyberFlood tests across a multitude of available platforms.
- **Avalanche Software Support—**Run the full breadth of Avalanche software on the CF20, providing maximum flexibility and test coverage.
- **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.

Technical Specifications		
Available Hardware Configurations		
CF20 with 2xQSFP28	8x10G Fan out 2x40G 2x100G	Cryptographic Acceleration Module QSFP28 transceivers not included
CF20 with 8x10G/8x1G	8x10G/1G SFP+ Cryptographic Acceleration Module Includes 8x10G/1G MMF SFP+ transceivers	
CF20 with 4x10G/4x1G	4x10G/1G SFP+ Includes 4x10G/1G MMF SFP+ transceivers Does not include Crypto Acceleration Module	
The CF20 with 2xQSFP28 interfaces is 25G and 50G capable with future license options		
The CF20 is capable of over 60Gbps of HTTP traffic generation capability on the QSFP28 model		
Software License Options		
Performance Testing Software	Comes with HTTP/HTTPS scale bandwidth, connectivity and rate testing, advanced mixed traffic testing custom traffic replay and DNS	
Security and Performance Testing Software	Comes with All CyberFlood options covering CyberSecurity Assessment for malware and attacks, DDoS testing and all performance testing software options	
TestCloud subscription	Allows options for always up-to-date download-able content for application scenarios, attacks/exploits and malware	
Advanced Fuzzing	CyberFlood provides powerful options for fuzz testing for common web protocols	
CyberFlood Feature Details		
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 20,000 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, end point services. Users can send attack over TLS sessions and apply evasions techniques to further stress security solutions detection capabilities	
Malware	Over 70,000 recent and zero-day malware samples including command and control behavior and binary malware transfer scenario	
DDoS	Test the DUT 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	
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 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 Bandwidth Tests	Find the maximum throughput achievable using emulated, realistic HTTP clients and HTTP servers and leveraging a configurable network topology	
HTTP 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	
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).	
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	

Technical Specifications (cont'd)	
Dimensions	(1U) 1.7" H x 16.8" W x 17.0" D; Fits standard 19" rack
Weight	17 lbs. (7.7 kg)
Operating Environment	5°C–35°C
Non-Operating Environment	0°C–50°C
Relative Humidity	10%–90% (non-condensing)
Power Requirements	115-230V, 50/60 Hz – 750W
Regulatory Approvals	FCC Part 15 Class A CE Mark Class A EN 55032:2012; EN 55024:2010; EN 61000-3-3:2013; EN 61000-3-2:2014

Ordering Information

Description	Part Number
CF20 10G/1G Performance Kit 8XSFP+	CF-KIT-011-CF20
CF20 10G/1G Security Performance Kit 8XSFP+	CF-KIT-012-CF20
CF20 100G/40G/10G Performance Kit 2XQSFP28*	CF-KIT-013-CF20
CF20 100G/40G/10G Security Performance Kit 2XQSFP28*	CF-KIT-014-CF20
CF20 10G/1G Performance Kit 4XSFP+	CF-KIT-015-CF20
CF20 10G/1G Security Performance Kit 4XSFP+	CF-KIT-016-CF20
CyberFlood Advanced Content Bundle: Attacks, Advanced Malware, TestCloud, Global IP	CF-CB-A-CF20-1Y
CF20 CyberFlood Advanced Mixed Traffic Assessment	CF-SW-ADV-CF20
CyberFlood Content Bundle: Attacks, Standard Malware, TestCloud, Global IP	CF-CB-CF20-1Y

Performance Kits Include: DNS Test Methodology, Throughput Mixed Traffic (Default Protocols), HTTP Open Conns Testing, Max Http Throughput Testing Methodology, Traffic Replay

Security Performance Kits Include: DNS Test Methodology, Throughput Mixed Traffic (Default Protocols), HTTP Open Conns Testing, Max Http Throughput Testing Methodology, Traffic Replay, CyberSecurity Assessment, Volumetric DDoS, Protocol DDoS

*QSFP28 Transceivers are not included.

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

Requirements

The client used to access the virtual host/CyberFlood controller 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

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

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 | 02/21