DATASHEET

CyberFlood Security Testing

Security Efficacy and Validation Solutions

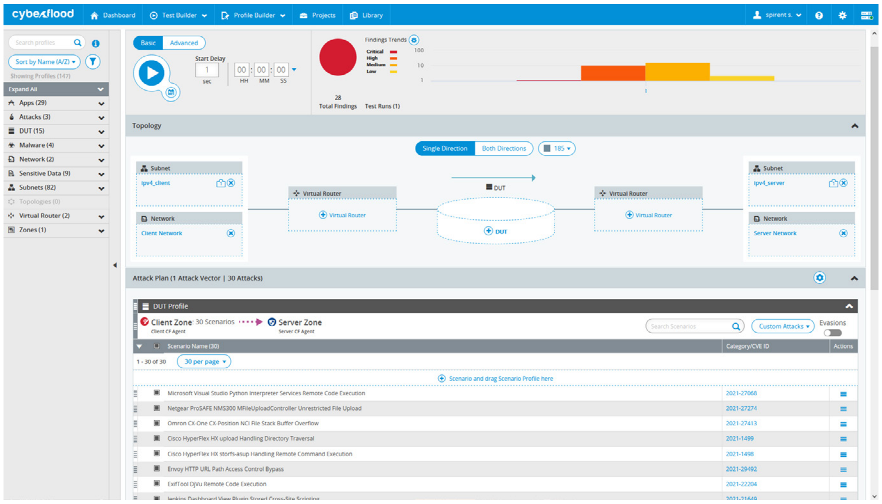
The deployment of a modern security and application-infrastructure brings with it innovative capabilities for managing traffic, security and Quality-of-Service (QoS) policies. However, to accurately test the security efficacy of application-aware infrastructures and devices, it is critical to emulate hyper realistic legitimate and hacker traffic to fully assess security controls are working to your specifications.

With many thousands of applications on the network and hundreds of new ones being released every day on millions of devices, QA, engineering and IT teams are struggling to quickly and effectively test, validate and roll-out their app-aware security architectures.

The Solution: CyberFlood

Security Testing—find and fix vulnerabilities quickly. The Spirent CyberFlood security testing options provide users an effective means to test with a database of tens of thousands of up-to-date application, attack, and malware scenarios. This allows you to mix attacks and applications to verify and analyze network security. You can add realistic hacker behavior with evasion techniques or encrypt attacks to push security solutions to their limits. For malware testing, CyberFlood provides infected host emulation, as well as malware binary transfer-based security testing. Plus, you can quickly create custom tests for unique protocols, traffic flows, and applications, without scripting, and leverage smart remediation tools to shorten the time to find and fix vulnerabilities.

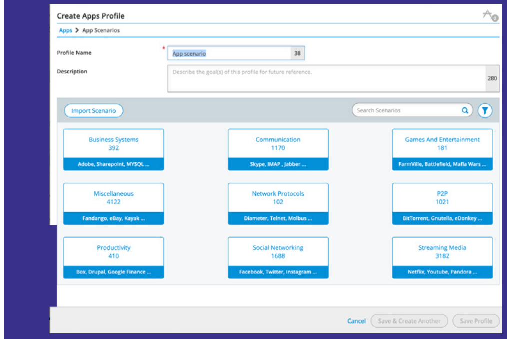
Delivered via the optional TestCloud content subscription, CyberFlood enables users to stay on top of the application explosion and easily recreate millions of sessions of real application traffic in the lab. Users can quickly test application performance and security detection and control capabilities of systems, such as next-generation firewalls, IDS/IPS, SD-WAN, SASE, DPI solutions, and more.



Scenario Name (30)	Category/CVE ID	Actions
Microsoft Visual Studio Python Interpreter Services Remote Code Execution	2021-27068	≡
Netgear ProSAFE NMS300 MFileUploadController Unrestricted File Upload	2021-27274	≡
Omron CX-One CX-Position NCI File Stack Buffer Overflow	2021-27413	≡
Cisco HyperFlex HX upload Handling Directory Traversal	2021-1499	≡
Cisco HyperFlex HX storfs-asup Handling Remote Command Execution	2021-1498	≡
Envoy HTTP URL Path Access Control Bypass	2021-29492	≡
ExifTool DjVu Remote Code Execution	2021-22204	≡
Jenkins Dashboard View Plugin Stored Cross-Site Scripting	2021-21649	≡

Overview

With the deployment of application-aware systems, such as application firewalls, SD-WAN, SASE, and DPI engines, the network is becoming more distributed and intelligent at the application level. With this awareness, the network elements' ability to implement intelligent traffic management, security, and Quality-of-Service (QoS) policies, that are tied to specific application and user characteristics, needs to be thoroughly validated. CyberFlood provides this validation support, as well as use of the MITRE ATT&CK™ framework, allowing users to model security validation using industry attack techniques and groups to better manage and fix vulnerabilities.



Profile Name * App scenario 38

Description: Describe the goal(s) of this profile for future reference. 280

Business Systems 392 Adobe, Sharepoint, MYSQL ...	Communication 1170 Skype, IMAP , Jabber ...	Games And Entertainment 181 FarmVille, Battlefield, Mafia Wars ...
Miscellaneous 4122 Fandango, eBay, Kayak ...	Network Protocols 102 Diameter, Telnet, Molbus ...	P2P 1021 BitTorrent, Gnutella, eDonkey ...
Productivity 410 Box, Drupal, Google Finance ...	Social Networking 1688 Facebook, Twitter, Instagram ...	Streaming Media 3182 Netflix, Youtube, Pandora ...

Flexibility

CyberFlood Security Testing is available as an option on all CyberFlood platforms: Appliances, Virtual and Cloud solutions.

Using tens of thousands of ready-to-run performance and security tests for a wide range of popular applications, including peer-to-peer (P2P), Business, Instant messaging (IM), Social Media, and thousands of known security attack templates, users can test:

- Policy Enforcement for QoS Application-aware systems, such as DPI engines, application firewalls, and mobile packet gateways.
- The effectiveness of DPI, IPS/IDS, ALG, SASE, and SD-WAN systems, evaluating their performance under real-world conditions, as well as the potential impact of security attacks on performance.
- Comprehensive multi-zone test cases to run applications, attacks and malware through multiple devices and security controls in the same test.
- DDoS mitigation services and policies with volumetric and protocol DDoS emulation.
- Advanced NGFW and SD-WAN security inspection capabilities with full support of application, attack and malware scenario encryption.
- Security controls via SNI policy detection scenarios.
- Devices with mixed legitimate load and attack traffic to further challenge and assess security controls under real-world conditions.
- Data loss prevention (DLP) policies, using CyberFlood files created on-the-fly or custom file sets, to quickly assess that those policies are working to your specifications.
- Security controls with encrypted content, including applications, attacks and malware, to validate the security controls' ability to manage encrypted legitimate and malicious content. Upload your own certificates for specific and comprehensive test configurations.

Benefits

Accuracy: Test with real user-generated traffic, as seen on your network, with detailed metadata that describes the user operation contained in each test for quick identification and resolution of issues prior to deployment.

Actionable Results: Quickly determine security controls' catch rate of tested attacks with the ability to see the exact point of detection in the attack/malware flow, precisely showcasing security effectiveness.

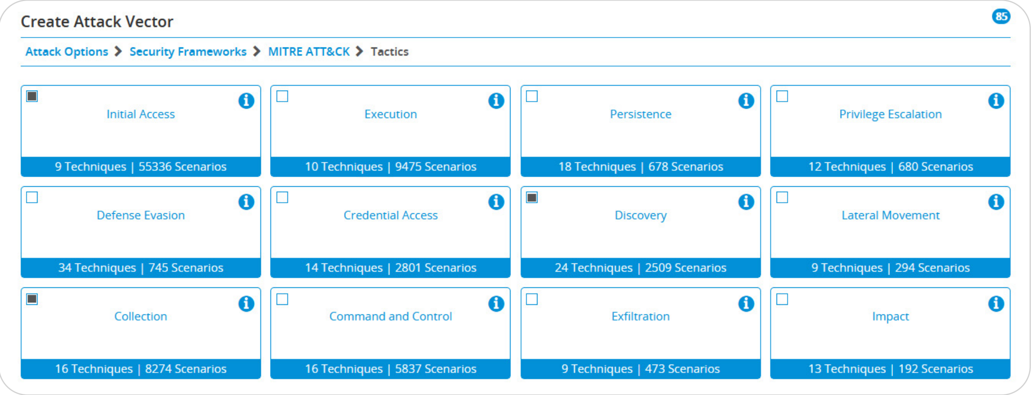
Live Content: Access content that is constantly updated with new application, attack, and malware scenarios to keep up with your dynamic environment and testing needs.

Flexible: Configure comprehensive application flows and define SNI header information that can be used to validate security controls for inspecting and identifying encrypted traffic.

NetSecOPEN: Test with built-in industry standard methodologies. NetSecOPEN is a network security industry forum of network security vendors, tool vendors, labs and enterprises, collaborating to create open and transparent testing standards for today's modern content-aware network solutions. CyberFlood Supports over 50 built-in NetSecOPEN methodologies.

MITRE ATT&CK™: Easily create and execute tests from the built-in MITRE ATT&CK framework. Quickly select from attack groups and techniques to validate specific vulnerability types. Use comprehensive MITRE ATT&CK reporting to quickly evaluate your security landscape.

Hacker Behavior: Easily add evasion techniques to further challenge security controls, with virtually unlimited traffic flow variants from a wide range of available evasion techniques.



Create Attack Vector

Attack Options > Security Frameworks > MITRE ATT&CK > Tactics

■ Initial Access 9 Techniques | 55336 Scenarios	□ Execution 10 Techniques | 9475 Scenarios	□ Persistence 18 Techniques | 678 Scenarios	□ Privilege Escalation 12 Techniques | 680 Scenarios
□ Defense Evasion 34 Techniques | 745 Scenarios	□ Credential Access 14 Techniques | 2801 Scenarios	■ Discovery 24 Techniques | 2509 Scenarios	□ Lateral Movement 9 Techniques | 294 Scenarios
■ Collection 16 Techniques | 8274 Scenarios	□ Command and Control 16 Techniques | 5837 Scenarios	□ Exfiltration 9 Techniques | 473 Scenarios	□ Impact 13 Techniques | 192 Scenarios

MITRE ATT&CK Group Selection

CyberFlood Security Testing Key Features

Real-world traffic: When the application content is replayed, it replicates (with precision) real user-generated traffic as seen on the network. Detailed metadata is provided per application test that describes the user operation contained in that test, such as login, chat, search, shared files, etc. These tests are created by recreating the interactions of real users on real devices as they use the relevant application.

For maximum flexibility, TestCloud is licensed separately for Application, Attack and Malware scenarios – choose the best solution for your testing needs.

Up to date: TestCloud is constantly updated to support the most popular applications in use and latest attack/malware scenarios. Customer requests, as well as end-user trends, determine the list of new applications that are added to TestCloud by Spirent. In addition, our attack library is frequently updated with fresh content, including zero-day attacks.

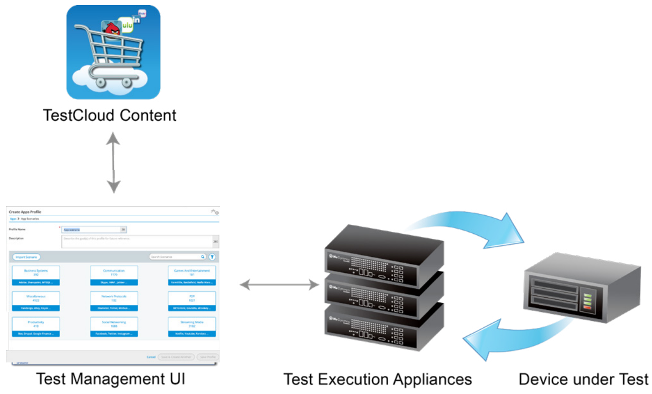
Vast database: Users access the largest repository of application tests and known security attacks in the industry, including multiple versions of applications, such as Skype, and multiple platforms, including iOS, Android, and Windows.

Attack/Malware scenarios: Multiple vectors are available, including Trojans, SQL injection, XSS, Worms, Virus, Spyware, Root Kit, File Infector, Adware, Bots, Backdoors, Key Loggers.

DDoS: Assess with a database of emulated volumetric and protocol DDoS with and without user traffic load to verify network device policy enforcement and mitigation capabilities.

Pre-defined mixes: Pre-configured sets of related applications and attacks are provided. Spirent TestCloud provides tens of thousands of ready-to-run performance and security tests for a wide range of popular applications, including peer-to-peer (P2P), Business, Instant messaging (IM), and Social Media. Examples of apps include BitTorrent, Facebook, Twitter, WhatsApp, Office 365, Skype and more.

SmartApps: The SmartApps editor allows users to edit real-world application scenarios and customize according to specific requirements, while taking advantage of Spirent's performance-oriented load engine to emulate real-world application traffic.



Ordering Information

Description	Part Number
CyberFlood Malware Content-1Yr	CF-C-ADVMALWARE-1Y
CyberFlood Attacks Content-1Yr	CF-C-ATTACKS-1Y
CyberFlood TestCloud Apps Content-1Yr	CF-C-TESTCLOUD-1Y
CyberFlood Protocol DDoS Option	CF-SW-PDDOS
CyberFlood Volumetric DDoS Option	CF-SW-DDOS
CyberFlood CyberThreat Assessment Option	CF-SW-CYBER

Other CyberFlood options are available for specific hardware, virtual and cloud platforms. Please contact Spirent Sales for more information.

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 C | 10/21 | www.spirent.com