Data Sheet

Spirent **CyberFlood**

應用程序和安全測試解決方案

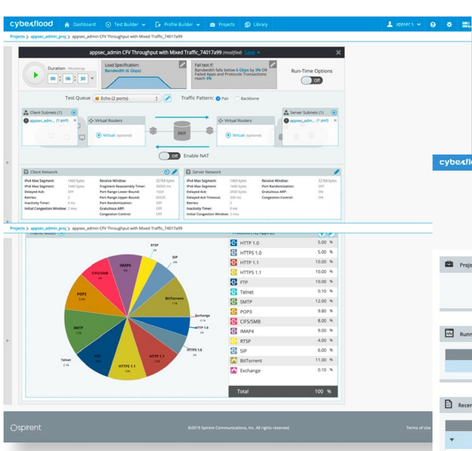
CyberFlood是一種功能強大且易於使用的測試解決方案，可生成數千種不同的實際應用程序流量場景和攻擊，以測試當今應用程序感知的網絡基礎架構的性能，可伸縮性和安全性。 與其他測試解決方案不同，CyberFlood根據實際的應用場景生成實際的高性能用戶應用程序，以進行實際的安全性，負載和功能測試。

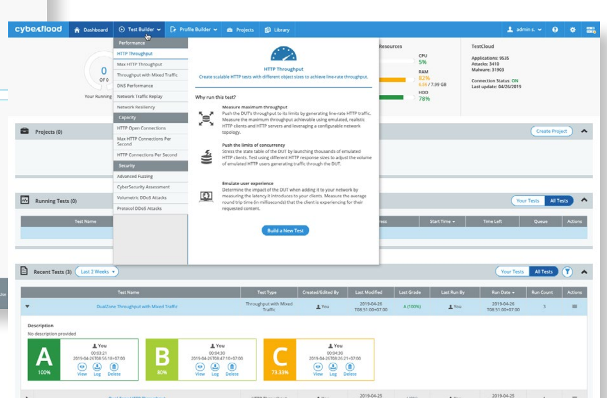
應用領域

CyberFlood通過幫助產品開發團隊以成熟的可擴展性，安全性和性能幫助他們更快地進入市場，從而為創建下一代內容感知設備和解決方案的產品開發團隊提供了競爭優勢。 企業和實驗室工程師可以確保他們部署的解決方案將提供所需的安全性。

借助CyberFlood，用戶可以快速，輕鬆地測試最新，最出色的應用程序和攻擊（不斷更新），並具有無與倫比的真實性和可擴展性。 用戶可以將他們的解決方案推到極限，同時確保基礎架構能夠滿足實際需求。

- **真實性-測試您的網絡，流量和現實情況：:** 測試可識別應用程序的設備時，至關重要的是應用程序組合應反映L2-7層的實際情況。 CyberFlood使您能夠通過捕獲真實用戶在真實設備上的交互來創建測試，因為他們使用網絡上的真實應用程序以前所未有的真實感進行測試。
- **敏捷性-現在進行測試，而不是幾個月後進行測試:** CyberFlood包括我們的TestCloud，使您可以訪問數千個隨時可以運行的性能和安全性測試，並能夠在出現新的應用程序或協議時立即創建新的測試。 從基於手機的應用程序到最新的P2P文件傳輸，CyberFlood擁有數千種用戶方案。 此外，您可以在幾分鐘內捕獲自己的網絡流量，並從一次流量捕獲中生成數百個自動化測試。
- **安全性-快速發現並修復漏洞:** Spirent TestCloud包含成千上萬的已知攻擊配置文件，因此您可以測試各種攻擊和應用程序組合，以驗證和分析網絡安全性。 對於惡意軟件測試，我們提供受感染的主機仿真以及基於惡意軟件二進制傳輸的安全性測試。 此外，您無需腳本即可快速為獨特的協議和應用程序創建自定義測試，並利用智能修復工具縮短修復漏洞的時間。
- **靈活性-滿足您需求的正確解決方案:** CyberFlood可在多種平台上使用，以滿足您的特定需求。 用於移動測試的便攜式解決方案，支持1G，10G，25G，40G，50G和100G本機速度的設備可提供更高的性能和容量，以及用於SDN / NFV設備和環境的無限測試的完全虛擬化的解決方案。





Spirent **CyberFlood**

應用程序和安全測試解決方案

特點與優勢

- **具有混合流量的吞吐量:** 使用預配置的流量混合來創建和運行測試，以實現高吞吐量SSL / TLS加密，或者從包含數千個應用場景的數據庫中創建自己的混合，並混入攻擊流量以驗證負載下的安全策略。
- **網絡安全評估:** 運行數以萬計的現代和高級攻擊，DDoS和惡意軟件（二進制傳輸和受感染的主機仿真）。
- **應用程序識別:** 使用TestCloud的1000多種應用程序創建大量最新的移動和雲應用程序，以及安全流量模式。我們的庫會不斷更新，可直接下載，以確保您擁有最流行且相關的應用程序和攻擊，可滿足您的測試需求。
- **大規模吞吐量:** 創建以1Gbps至100Gbps速率運行的測試，以突破運營商級設備和網絡服務的界限。
- **專案項目:** 創建具有共同目標的測試組，以供多個團隊成員進行工作，從而大大提高測試實驗室的效率。
- **流量重播:** 從您自己的環境中重播並擴展捕獲的流量重現條件。按原樣重播大文件，以保持原始流量保真度，或修改流量。此外，覆蓋捕獲的流量上的IP和MAC地址以在新條件下進行測試。
- **每秒大規模連接:** 快速創建測試以驗證設備或網絡可以處理的加密和/或非加密容量。
- **基於SmartMutation™的模糊處理:** 執行不同的服務和協議突變方案（包括服務器響應模糊處理）以發現漏洞並通過動態創建的數百萬次測試迭代來測試已實施協議的可靠性。 定義要測試的協議組件。 重複精確的模糊迭代以重現故障事件。
- **可靠性測試:** 對TestCloud應用程序負載執行長時間的浸泡測試，以確保解決方案能夠長時間以高容量工作。
- **NetSecOPEN:** NetSecOPEN是一個網絡安全行業組織，網絡安全供應商，工具供應商，實驗室和企業在其中協作以創建開放和透明的測試標準。
- **Global IP 選擇器:** 通過選擇地圖上的全局區域，快速選擇在何處創建模擬流量。

平台選項

- **C1 Portable Appliance**
  4 x 1G, 2 x 10G and 4 x 1G and 2 x 10G options
- **CF20 1U Self Contained Appliance**
  4 x 1G, 8 x 1G, 8x10G, 2 x 40G, and 2 x 100G interface options
- **C100-S3 High Performance Appliance**
  16 x 1G, 8 x 10G, 16 x 10G, 4 x 25G, 4 x 40G, 4 x 50G, 4 x 100G options
- **C200 Slim-lined Ultra Performance Appliance**
  8 x 10G, 16 x 10G, 4 x 25G, 4 x 40G, 4 x 50G, 4 x 100G options
- **CyberFlood Virtual**
  ESXi or KVM instances–靈活的可擴展性
- **Amazon AWS, Azure, and Google Cloud (GCP)**
  在雲環境中使用的部署

系統要求

客戶端–用於訪問虛擬主機的客戶端必須滿足以下最低要求才能運行CyberFlood：運行最新瀏覽器版本（2017年6月或更高版本）的任何Windows，Mac或Linux PC；Firefox瀏覽器，Google Chrome瀏覽器

虛擬主機–用戶提供的虛擬主機系統必須滿足以下最低要求才能運行CyberFlood虛擬主機軟件

- VMware vSphere Hypervisor ESXi–(v5.1.0 or higher, 64-bit only, bare metal)
- KVM on Linux–(64-bit only, bare metal)
- 128G Hard Drive
- 8G RAM
- 2+ GHz Dual Core Processor (64-bit)
- VT extensions enabled for 64-Bit OS
- Dedicated network interface with a static IP address

訂購信息

Description	Part Number
CyberFlood Base License for C100	CF-SW-BASE
CyberFlood Cyber Security Suite	CF-SW-CYBER
CyberFlood Volumetric DDoS Suite	CF-SW-DDOS
CyberFlood Dns Test Methodology	CF-SW-DNS
CyberFlood Emix Tests–Throughput with Mixed Apps	CF-SW-EMIX
CyberFlood HTTP Open Conns Testing Methodology	CF-SW-HCONNS
CyberFlood Max HTTP Throughput Testing Methodology	CF-SW-HMAX
CyberFlood Protocol DDoS	CF-SW-PDDOS
CyberFlood Traffic Replay	CF-SW-TRAFFREP
CyberFlood Advanced Malware Content-1Yr	CF-C-ADVMALWARE-1Y
CyberFlood Attacks Content-1Yr	CF-C-ATTACKS-1Y
CyberFlood Standard Malware Content-1Yr	CF-C-MALWARE-1Y
CyberFlood TestCloud Apps Content-1Yr	CF-C-TESTCLOUD-1Y
CyberFlood CyberSiege Global IP Traffic Selector-1Yr	CF-SW-IANA-1YR

其他CyberFlood選項可用於特定的硬件平台和Advanced Fuzzing選項，請聯繫Spirent銷售以獲取更多信息。

聯繫我們

有關更多信息，請致電您的思博倫銷售代表或

請訪問我們的網站：www.terilogy.com.tw/Spirent

www.terilogy.com.tw

Taiwan
| sales@terilogy.com.tw