



SPIRENT STUDIO SECURITY

NETWORK SECURITY USING REAL THREATS AND APPS

Security threats are on the rise and costing millions of dollars in lost business to service providers, enterprises and government agencies. New threats in the form of worms, viruses, malware, vulnerabilities and DDoS attacks are being discovered daily. According to Symantec, there were over 3 billion malware attacks in 2010 alone.

With the growth and adoption of technologies like TCP/IP, Ethernet and the Web, network infrastructure is more open and accessible than ever before making it easier for widespread damage to occur. Areas such as Unified Threat Management (UTM), Cyber Security, Cloud services, Critical Infrastructure, Unified Communications and Enterprise Storage are all seeing rapid growth using these technologies, yet at the same time they are exposed to a sophisticated and growing list of persistent threats including cyber attacks, data ex-filtration and malformed traffic. With millions of applications, devices and users active on the network and thousands of attacks being discovered every day, test teams are struggling to quickly and effectively test the security aspects of their systems and networks.

Legacy test tools are ineffective in meeting today's security testing challenges offer limited point solutions, rudimentary defect resolution capabilities and requiring a high level of security expertise.

Spirent Studio Security is the industry's only unified security testing solution designed for testing today's network infrastructure. For the first time users can test in a single unified platform designed for all their security needs, leverage a suite of tests comprised of millions of test cases to exhaustively cover all possible production conditions and enjoy an easy yet powerful workflow that shortens the time to fix defects. The solution allows users to quickly create custom tests for unique protocols and applications without scripting and provides remediation tools for faster reproduction of defects by developers.

APPLICATIONS

- Measure the ability of the network device to detect and prevent thousands of known attacks
- Test the resiliency of the network device by verifying its ability to deal with millions of unexpected and malicious inputs
- Test the reliability of a network device by generating negative tests for virtually any protocol interaction including custom protocols and proprietary extensions
- Measure the ability of the network device to withstand targeted DDoS attacks
- Test the capabilities of the target to inspect traffic for malware, unwanted URLs and spam and take appropriate action

BENEFITS

- Protect against the latest known security attacks
- Prevent costly downtime by discovering weaknesses before deployment
- Prevent field-driven fire drills

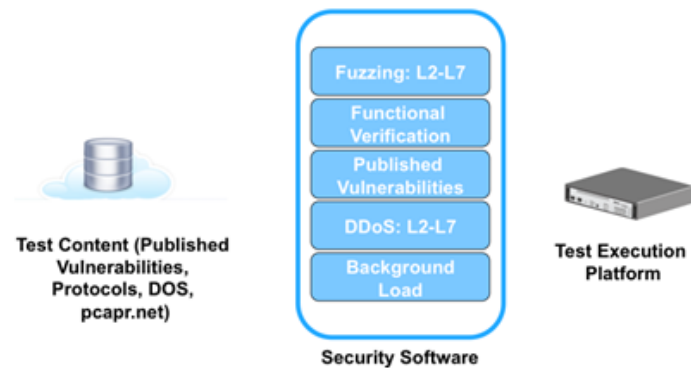
SPIRENT STUDIO SECURITY

NETWORK SECURITY USING REAL THREATS AND APPS

ARCHITECTURE

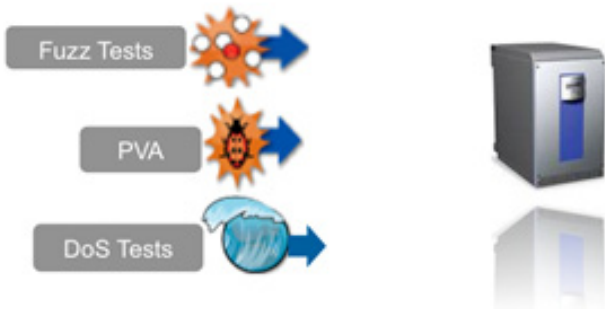
Spirent Studio Security is made up of the following key components:

- **TestCloud:** An integrated cloud-based store containing thousands of application tests and security attacks, with hundreds posted new each month
- **Test Management Server:** The software for managing security testing, delivered as a virtual machine (VM) for immediate deployment
- **Text Execution Appliances:** Rack mountable appliances that generate the application traffic at production network throughputs. Support models include Mu-8000 and Mu-8010



KEY FEATURES

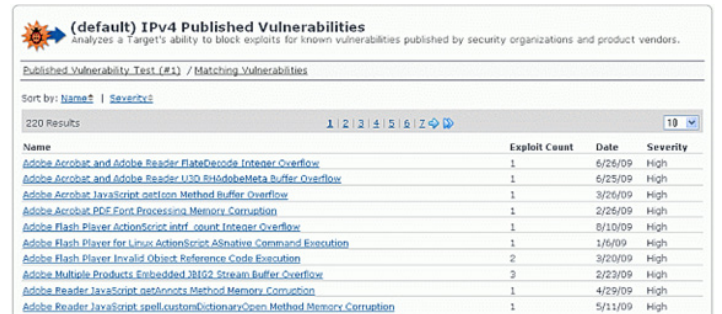
- **Fuzz testing:** Fuzz testing is the most effective way to run negative tests for unexpected inputs and events. This method helps improve robustness and reliability by testing for unexpected, negative test cases that often cause catastrophic and costly crashes or failures on the live network.





- **DDoS replication:** Quickly replicate a large variety of actual and potential DDoS attacks to test the resiliency of applications and services



- **Published Vulnerabilities:** The Published Vulnerabilities (PV) Module offers a continuously growing and up-to-date list of software vulnerability triggers, which mirrors the latest real-world attacks found in the wild on the Internet.



- **Security Capability Verification:** Security features such as malware detection and prevention, URL filtering, white-listing and black-listing of applications can be easily tested using spreadsheet-based data-driven testing.
- **Monitors:** The rich set of monitors interact with the target to help isolate and reproduce faults. Monitors include protocol health checks, SNMP monitors, SSH and Telnet based command monitors, remote log monitors and console monitors.
- **Remediation Tools:** Helps testers collaborate with developers to reduce defect resolution time by providing a remediation toolkit for each identified fault. The toolkit enables developers to quickly reproduce faults in their environment before re-testing and validating the fix.
- **Test Automation:** The solution is designed for automation with a rich set of API interfaces that can be accessed from a TCL, Python, Perl or other similar automation frameworks. The solution can also be set into a mode that enables lights-out testing, automatically restarting targets if they crash during a test run.

STUDIO SECURITY SOFTWARE SPECIFICATIONS	
Protocols	DDoS, published vulnerabilities (PVA), scalability, verification, fuzz testing
STUDIO SECURITY HARDWARE SPECIFICATIONS—MU-8000, MU-8010	
Chassis	2U, 19" rack-mount 3.5 x 17 x 20 in. (8.9 x 43.2 x 50.8 cm.)
Weight	29.5 lbs. (13.38 kg)
Power	115 to 240V AC, 50 to 60Hz, 8Amp-4Amp
Power Relays	10Amp/250V power relay fuse
Storage	(2) hard drives, 2.5", 10000RPM
Environmentals	<ul style="list-style-type: none"> • Operating temperature 14 to 100° F (-10 to 38° C) • Storage temperature 22 to 158° F (-30 to +70° C) • Operating or storage relative humidity 10 to 95%, non-condensing
Connectors	<ul style="list-style-type: none"> • (2) Ethernet (10/100/1000 Mbps auto-negotiating, RJ45) • (2) Serial console ports (RS-232 D89) • (2) Power relay ports • (2) USB ports • (2) ExpressCard 54 slot (reserved for future use)
Test Ports	<p>Mu-8000 Appliance (as shipped)</p> <ul style="list-style-type: none"> • (4) Ethernet (10/100/1000 auto-negotiating, RJ45) • (4) Gigabit SFP (1 Gbps, multi-mode, non-negotiating, fiber); PHY is IEEE 802.3 1000GBASE-SX <p>Mu-8010 Appliance (as shipped)</p> <ul style="list-style-type: none"> • (4) Gigabit SFP+ (10 Gbps, multi-mode, non-negotiating, fiber); PHY is IEEE 802.3 10GBASE-SR • (4) Gigabit SFP (1 Gbps, multi-mode, non-negotiating, fiber); PHY is IEEE 802.3 1000GBASE-SX
Agency Approvals	<ul style="list-style-type: none"> • CE Mark, FCC Part 15 Class A • Underwriters Laboratories <div style="display: inline-block; vertical-align: middle;">   </div>

SPIRENT SERVICES

Spirent Global Services provides a variety of professional services, support services and education services—all focused on helping customers meet their complex testing and service assurance requirements. For more information, visit the Global Services website at www.spirent.com or contact your Spirent sales representative.

SPIRENT STUDIO SECURITY
NETWORK SECURITY USING REAL THREATS AND APPS

Developed by  **Mu Dynamics**

AMERICAS 1-800-SPIRENT • +1-818-676-2683 • 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

© 2012 Spirent Communications, Inc. All of the company names and/or brand names and/or product names referred to in this document, in particular the name “Spirent” and its logo device, are either registered trademarks or trademarks pending registration in accordance with relevant national laws. All rights reserved. Specifications subject to change without notice. Rev. A 05/12

