



## Vulnerability Assessment

# AVALANCHE VULNERABILITY ASSESSMENT TESTING SOLUTIONS

In today's hostile computing environment, companies are justifiably concerned about suffering attacks from malicious entities. Distributed Denial of Service (DDoS), ConFlickr worm, Nimda, SQL Slammer, email viruses and their endless variants — IT professionals understand that defending against these attacks is a difficult proposition, and that the price of failure is higher than most companies are willing to admit.

Avalanche Vulnerability Assessment emulates thousands of attacks and variants including:

- DDoS
- Worms
- E-mail attacks
- Viruses / Trojans
- VoIP attacks
- Application penetration
- Evaded Attacks
- Additional emulations become possible with the continuous release of new exploit definitions and threat updates

Avalanche's Vulnerability Assessment next-generation solution provides visibility into essential areas of network security and allows Spirent customers to move beyond just measuring the network's capacity for normal traffic. Customers can now emulate and analyze the effects of corrupt and malicious traffic and other impairments on their networks alongside normalized user traffic.

By using Avalanche's Vulnerability Assessment, network security professionals can identify vulnerabilities through realistic attacks on individual devices or entire networks. The ability to run sequences of controlled attacks (even timing attacks throughout an entire test run) greatly accelerates the task of closing system vulnerabilities and setting the right security policies. Continuously updated exploit definitions in the Avalanche Attack knowledge base assist in the prevention of malware surprises.



Avalanche 2900

### DON'T FACE THE THREAT ALONE

Avalanche is the industry leading layer 4-7 test solution for emulating millions of users for testing content aware networks and devices. In the mix of normalized traffic are the undercurrents of threats and traffic anomalies that can be difficult to assess and address. By incorporating the power of Spirent's ThreatEx attack generation solution into Avalanche you now have a consolidated and powerful ally in the ongoing battle to defend your network against malicious traffic and tighten your security counter measures. Some benefits of this solution include:

- Closes the window of vulnerability and reduces the need for in-house research by providing threat updates as soon as new outbreaks occur
- Enhances lab-based vulnerability testing by injecting hostile traffic in conjunction with normalized (good) traffic
- Enables IT personnel to confirm vendor performance claims by assessing network defenses against known and unknown threats
- Features diagnostic, assessment and reporting capabilities
- Provides a proactive threat-containment strategy, reducing the risk of costly network downtime
- Allows testing of robustness for next generation UTM (Unified Threat Management) Systems and other advanced security mechanism, verifying their capability under mixed attack and high volume normal traffic conditions

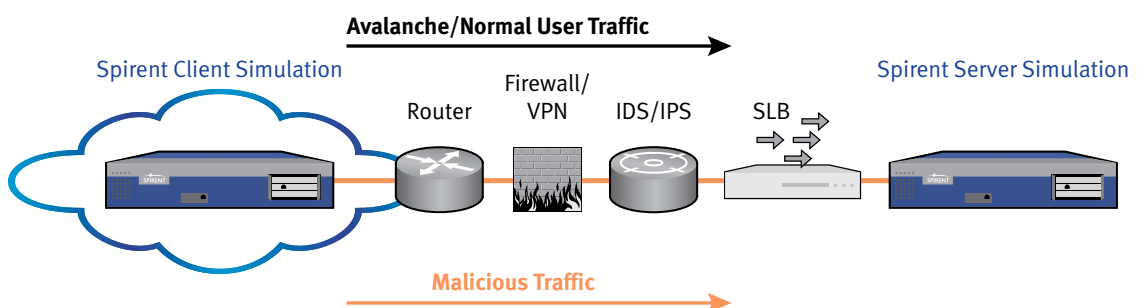
### AVALANCHE ATTACK KNOWLEDGE BASE AND UPDATE SERVICE

To ensure you are fully protected against the latest threats, Spirent offers a subscription based threat definition update service for the Avalanche solution. Subscription to this database ensures your QA and IT staff have immediate access to the latest threat signatures, delivering zero-day testing capabilities. Avalanche attack knowledge base updates can be downloaded at the end of each business day or pulled down as needed.



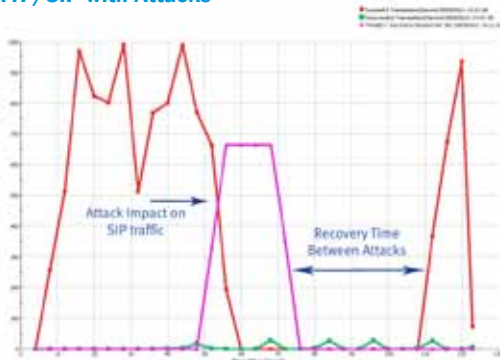
### AVALANCHE ATTACK DESIGNER

Avalanche Attack Designer enables IT and QA staff to modify existing threats or to create customized threats in minutes – without time-intensive programming. The intuitive point-and-click graphical user interface enables threats and exploits to be developed simply by describing them. The software then generates exploits using a patented TDL (Threat Definition Language) format. Users can also import specific traffic via Pcap files and replay or modify unique protocols or other transactions. Threat files can be executed directly by the Avalanche system or stored in a central database for future use.



Adding Avalanche Vulnerability Assessment to existing test methodologies Enables IT and QA staff to use mixtures of both positive and negative traffic to test the security infrastructure under load and will determine the absolute cause and effect of attack mitigation.

#### HTTP/SIP with Attacks



**AUTOMATION** - To streamline and automate the testing process Avalanche provides a complete TCL API so QA staff can select export Avalanche test plans to TCL or develop an entire test through the API. This automated approach simplifies the process of re-testing the network each time a new threat is detected. Developers can configure test parameters, threat parameters and statistical monitoring techniques through an intuitive GUI, and automatically generate Tcl scripts to be executed.

**AN END-TO-END SOLUTION** - Avalanche Vulnerability Assessment delivers a complete negative traffic testing assessment solution to protect your network from hostile attacks. By adding Vulnerability Assessment testing to you standard methodologies your company gains more than access to the market-leading testing platform for malicious attacks. You also get a full and active partner constantly on the alert for new threats. Don't go at it alone – deflect hostile network threats by using Avalanche Vulnerability Assessment

**MULTI-PLATFORM SUPPORT** - Avalanche Vulnerability Assessment will work on all current hardware platforms available today for Avalanche to address various testing needs. ThreatEx will run Avalanche 290 and 2900 Appliances or the Spirent TestCenter™ multi-slot chassis for maximum versatility. The Avalanche 290 is perfect for smaller bench level applications needing up to 2Gbps of bandwidth and the Avalanche 2900 provides multi port 1Gbps scale up to 10Gbps interfaces appliance delivering maximum performance. For added flexibility, scalability and complete assessment capabilities, Avalanche Vulnerability Assessment will also run on the multi-slot Spirent TestCenter chassis and all Avalanche compatible HyperMetrics test modules. Doing so expands the test bench to include threat capabilities to the many other applications supported on the Spirent TestCenter.

#### Avalanche Vulnerability Assessment - Appliances

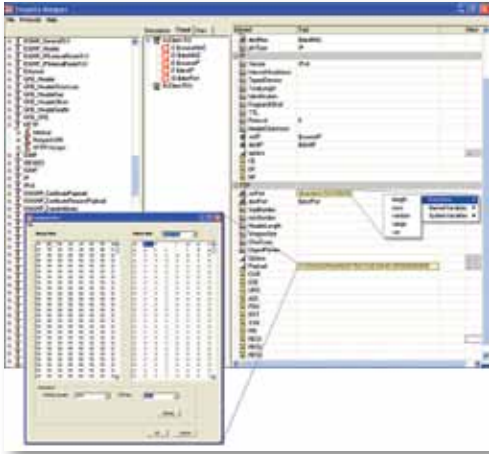
##### Ordering Information

Description	Part Number
Avalanche Vulnerability Assessment Option for Avalanche 2900 1G to 10G solutions	CEE-SW-VA
Avalanche Vulnerability Assessment Option for Avalanche 290 Portable 1G	CEE-SW-VA-PT
Avalanche Vulnerability Assessment Attack Knowledge Base 1Yr Subscription	SUB-0001

#### Avalanche Vulnerability Assessment - Spirent TestCenter

##### Ordering Information

Description	Part Number
Avalanche Vulnerability Assessment Option for Avalanche on Spirent Test Center – HyperMetrics CM modules - 9U chassis	BPK-1089A
Avalanche Vulnerability Assessment Option for Avalanche on Spirent Test Center – HyperMetrics CM modules - 2U chassis	BPK-1089A-2U
Avalanche Vulnerability Assessment Option for Avalanche on Spirent Test Center – HyperMetrics AP modules - Per Module	BPK-1089A-CPU-MOD
Avalanche Vulnerability Assessment Attack Knowledge Base 1Yr Subscription	SUB-0001



Avalanche Attack Designer enables you to control the attributes of any threat, and embed any payload into the protocol stream without programming.

### **SPIRENT GLOBAL SERVICES**

Spirent Communications understands that internal resources for managing complex testing programs may not always be available. Our Global Services engineers enable your business to quickly implement field-proven solutions, instead of spending time and resources to develop them in-house. Further information can be found at [www.spirent.com/gs](http://www.spirent.com/gs).

- **Avalanche Implementation Service:** Spirent can help you manage all facets of installing the Avalanche solution into your test bed – from site readiness analysis to physical installation and systems configuration. Knowledge transfer services are also available to help your staff perform critical testing tasks without delay
- **Network Security Assessment:** Experienced engineers from Spirent Global Services are available to assist in network vulnerability and performance assessment. Regulatory compliance can be established, and costs can be controlled by right-sizing your network security infrastructure
- **Engineering Services:** In-house access to Avalanche product experts can reduce your company's overall risk and accelerate the delivery of custom functionality. Additional resources translate into quick ramp-up, development, testing and deployment of customized attacks and protocols



Spirent Communications  
1325 Borregas Avenue  
Sunnyvale, CA 94089 USA

**SALES AND INFORMATION**  
[sales-spirent@spirent.com](mailto:sales-spirent@spirent.com)  
[www.spirent.com](http://www.spirent.com)

**Americas**  
T: +1 800.SPIRENT  
+818 676.2683

**Europe, Middle East, Africa**  
T: +33 1 6137.2250

**Asia Pacific**  
T: +852 2511.3822