



Contact:  
Kevin Gallagher  
Gallagher Group Communications  
925.831-1041  
[kevin@gg-comm.com](mailto:kevin@gg-comm.com)

## **MU SECURITY AND NSP COMPLETE SERVICE PROVIDER TCO AND ROI STUDY**

### **Study Details Service Provider Best Practices for Avoiding Network Downtime and Customer Churn; Dec 6 Webcast and Web-based ROI Calculator Available**

**Sunnyvale, Calif. – November 15, 2007** – Mu Security, the leader in network security analysis systems, today announced the completion of a new “*Total Cost of Ownership*” study for Service Providers and network vendors by Analyst Peter Fetterolf of Network Strategy Partners (NSP). The study, conducted during the past nine months, features four case studies of leading global providers using the Mu-4000 appliance to uncover the often hidden metrics of revenue loss due to customer churn, network robustness issues and downtime. NSP and Mu Security also leveraged this new primary research to create an online calculator site: <http://www.musecurity.com/solutions/calculator.html>..

Mu Security and NSP will host a Webcast on Thursday, Dec. 6 at 8:00 a.m. PST to discuss how customers like Cox Communications are improving networked application or service availability and reliability by addressing robustness and resiliency factors before any networked product is deployed into a production environment. The interactive TCO & ROI calculator, whitepaper, and webcast specify both “Service Provider Costs for Downtime and Churn” and “Service Provider and Developer Savings (Test & Certification).” All content and Webcast registration is available online at: [www.MuSecurity.com/solutions](http://www.MuSecurity.com/solutions).

“Many service providers we interviewed face unacceptable levels of downtime or customer churn due to network robustness issues,” said Fetterolf. “Survey participants found that integrating product robustness analysis to discover and eliminate weaknesses

and vulnerabilities reduces downtime and customer churn. In more than one instance, participants noted that the integration of robustness negative analysis into their deployment and development processes paid for themselves in less than a month by reducing customer churn or field fire drills.”

### **ROI and TCO Study Highlights**

The new study found that with existing analysis techniques, many network robustness issues go undetected until the worst case scenario happens and network downtime or malicious access occurs. Simply put, existing analysis techniques provide limited value. Most cover only the “shallow end” of the product’s communication attack surface “pool” through homegrown scripts, use of commercial stateless protocol fuzzing software and other open-source tools to test for security weaknesses. The problems found with manual testing are relatively obvious; many subtle system weaknesses and security flaws went undetected. VoIP system flaws—for example, in Session Initiation Protocol (SIP)—would have resulted in serious denial-of-service conditions in the production Internet telephony networks equating to opportunities for expensive network service outages.

Another study finding was the desire to virtualize the user’s specialized security incident response group through the automation engine of a Mu-4000 analyzer. Service providers all wanted the ability to define testing criteria and disseminate sharable security analysis templates to the rest of the organization to ensure common best practices. With this streamlined process, the efficiency of the organization as a whole has been improved.

### **Mu Helps Automate Robustness and Reliability Analysis**

This month Mu Security released its next generation security and robustness analyzer solution with new features including sharable analysis templates, interactive graphical response time charting and dynamic stateful protocol fuzzing as the basis for robustness analysis. Two customers, Cox Communications and Redback noted their particular use cases on eliminating product downtime, customer churn and ensuring the highest possible product quality.

“In order to provide our customers with the highest quality service and reliability, we use the Mu-4000 to ensure the equipment deployed on our network is thoroughly tested prior to placing it into production,” said Paul Farley, director of network intelligence & security engineering at Cox Communications. “Using the Mu-4000 to run virtually every conceivable testing scenario helps us live up to our customers’ expectations as their trusted provider of voice, video, data and wireless services.”

“As a leading provider of products used in the world’s largest triple-play networks, Redback assures its carrier customers the highest levels of security for critical applications that require robust performance,” said Rod Couvrey, vice president of software engineering at Redback. Mu Security and their innovative Mu-4000 appliance help ensure that the Redback software engineering team leverages security analysis as a best practice to identify and remediate possible product vulnerabilities or quality issues as early as possible in our development lifecycle.”

TCO and ROI Study participants received no compensation or special consideration to participate. Both service providers and their vendors were provided a set of 10 audience-specific questions and asked to reply via one-hour interview within 30 days including metrics specific to their analyzer installation.

### **About Mu Security**

Mu Security offers a market-leading security analysis system, delivering a rigorous and streamlined methodology for verifying the robustness and security readiness of any IP-based product or application. Founded by pioneers of intrusion detection and prevention technology, Mu Security is backed by preeminent venture capital firms including Accel Partners, Benchmark Capital and DAG Ventures. The company is headquartered in Sunnyvale, CA. For more information, visit the company's website at <http://www.musecurity.com>.

###