

# Finding Hidden Dangers.



 **Mu** Dynamics™

# Service Providers

SERVICE OUTAGES? NETWORK DOWNTIME? CUSTOMER CHURN? LOSING TO COMPETITION?

## Businesses Run on Fragile Networks

More and more mission-critical NGN applications are relying upon IP-based systems. These systems are highly interconnected, and many are built on increasingly open, standardized communication protocols and software. Unfortunately, with complexity comes the high cost associated with ensuring these systems are always reliable, available and secure. Networked applications and products, including perimeter security systems (e.g., firewalls, IDS's, UTMs, etc.), fail in production environments due to security, reliability or availability issues. These failures manifest themselves in the form of either outright system crashes or as poor response time that affects service availability. The latter type of "soft" faults often goes undetected, and is traditionally very difficult to isolate and fix. In addition, real-world scenarios like distributed Denial of Service attacks cause an unacceptable degradation in service quality ultimately resulting in lost revenue. A TCO/ROI study by NSP Partners and Mu documented that Tier 1 VoIP operators experience downtime costs in excess of \$100,000/hour: <http://www.mudynamics.com/solutions/calculator.html>.

## Existing Tools are Not Proactive

Network operators want to eliminate all types of network weaknesses to avoid service degradation, but ensuring reliability, availability, and security of IP-based systems without Mu's automation framework is difficult. Until now, service providers have lacked effective processes to help them offer more robust services. Existing system analysis frameworks have a few major limitations:

- **Depth:** not able to find significant percentage of operational weaknesses in systems;
- **Agility:** not able to keep up with the pace of product development and deployment;
- **Breadth:** not able to provide thorough coverage.

## Mu's Proven Solution Boosts Service Availability

To address these limitations, Mu Dynamics develops and produces a proactive service assurance solution to help customers systematically address even the most deep-seated robustness issues before systems are deployed in production environments. Leading network operators worldwide have come to rely on Mu's solution to build infrastructures that are resilient enough to sustain an acceptable quality of experience (QoE), even in the face of the most challenging real-world scenarios.



*Figure 1: An example of a response-time spike (soft fault) and a subsequent system crash (hard fault), where the red dot denotes the crash.*

*"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."*

Paul Farley, Director of Network Intelligence & Security Engineering, Cox Communications

*"...Mu Dynamics' solution has become indispensable to users who are methodically identifying the root causes of robustness shortcomings or deep-seated weaknesses in any IP-based product or service."*

Mike Monticello, Security Analyst, Enterprise Management Associates

## Case Study: A Major Cable Service Provider (MSO)

A major U.S. cable triple-play multi service operator actively uses Mu's solution to automate the service assurance analysis of their revenue-critical network applications - and has achieved many business benefits including lower customer churn and increased application uptime.

### Challenge: Robustness Issues Went Undetected

The experts at this Cable MSO previously used homegrown scripts and ad-hoc usage of open-source tools to assess their systems' weaknesses. The problems they found with manual testing were relatively obvious; many subtle implementation flaws went undetected.

### Benefit: 10x Test Coverage

With Mu's proactive service assurance solution, the Cable MSO estimates having achieved TEN TIMES GREATER system analysis coverage compared to their older, manual approach. Using the Mu-4000,

the Cable MSO found service-affecting flaws in critical VoIP network elements. These availability and security flaws would have resulted in serious denial-of-service conditions in the production network equating to opportunities for expensive network service outages that would have resulted in increased customer churn.

### Challenge: Scarce Domain Knowledge in Silos

In the past, a small, specialized incident response group did all domain-specific service assurance testing. In this example, the Cable MSO used to employ three staff experts who spent 20-40% of their time on manual security analysis. These are expensive resources and they are difficult to attract and retain. Not surprisingly, the larger product certification organization did not have sufficient expertise to isolate or remediate security issues, much less availability or reliability. Without the Mu-4000's automation capabilities, it would have

been effectively impossible to add business and operational metrics to this organization's processes.

### Benefit: Knowledge Dissemination and Best Practices

By handing off the "heavy lifting" of network analysis to the Mu-4000 system, the security group builds best-practice templates to first define acceptance criteria, then disseminate shareable security analysis templates throughout the organization to ensure common best practices and baselines. By adopting these streamlined processes, the efficiency and effectiveness of the whole organization has improved.

### Benefit: Finding Bugs Early Saves Time and Money

The Cable MSO also uses the Mu-4000 as a reliability, availability and security baseline for new product evaluation and bake-offs. By identifying potential weaknesses as early as possible in product selection, it saves time and money in service deployment.

# Software and Hardware Vendors

QUALITY ISSUES? EXCESSIVE FIELD FIRE DRILLS? LACK REPEATABLE PROCESS? NEED QUALITY METRICS?

## Vendors Are in a Bind

In the never-ending race to offer more features at a faster pace, vendors of software or hardware products often lack tools for ensuring high quality for their increasingly complex products and applications. Accelerated use of open-source software and outsourced development further exacerbate the problem making system level analysis ever more important. The pace of development has increased but test tools have not kept up.

## Production Bugs are the Most Expensive to Fix

The cost of finding and fixing bugs in a shipping product, once deployed, is several orders of magnitude higher than fixing bugs before the product's release, because:

- Systems engineers must engage the customer to identify the problem;
- Customer support must reproduce the bug;
- Sustaining engineers must isolate and fix the bug including full regression analysis.

NIST estimates it is 30-50x cheaper to fix a bug in development than in the field: <http://www.nist.gov/director/prog-ofc/report02-3.pdf>.

## Solution to Better Product Quality with Proven ROI

Mu's proactive service assurance solution improves product quality without slowing down the product development process. The result is a greatly reduced rate of field fire drills and product delays caused by avoidable quality issues. Vendors achieve significantly higher test coverage, much reduced cost of finding and fixing bugs, and lower customer support costs, which all translate to measurable ROI.

Mu's solution helps vendors methodically identify and fix bugs earlier in the development life cycle, and provides vendors with an automation framework for easy integration into existing processes, including regression testing. Furthermore, the solution enables vendors to demonstrate quality commitment to their customers via a repeatable process and tangible metrics.

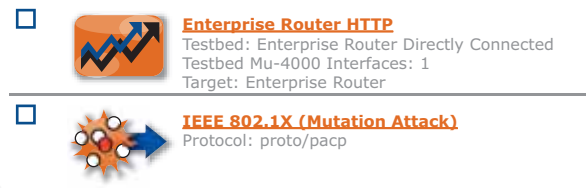


Figure 2: Sample sharable analysis templates.

*"The Mu-4000 helps ensure F5 products and updates are battle tested well in advance of commercial shipment."*

Patrick Jenny, VP of Development, F5 Networks

*"Mu's analyzer complements our internal vulnerability detection methods, which accelerates our remediation efforts, and decreases exposure to exploitation."*

Joe Levy, Chief Technology Officer, SonicWALL

*"As a leading provider of products used in the world's largest triple-play networks, Redback assures its carrier customers the highest levels of reliability, availability, and security for critical applications that require robust performance. Mu Dynamics and their innovative Mu-4000 appliance help ensure that the Redback software engineering team leverages service assurance methodologies as a best practice to identify and remediate possible product weaknesses or quality issues as early as possible in our development lifecycle."*

Rod Couvrey, Vice President, Software Engineering  
Redback Networks

## Case Study: SonicWALL

SonicWALL, a leading firewall product manufacturer, uses the Mu-4000 to improve their product's IDP signature capabilities to block network-borne vulnerabilities.

### Benefit: Significant Savings in Just One Month

SonicWALL calculated the Mu-4000 PAID FOR ITSELF IN ONLY ONE MONTH. The cost savings was due to a combination of reduced testing costs and soft dollar savings associated with finding product quality problems before its appliances are deployed in production networks. SonicWALL is painfully aware that quality problems in production networks may result in negative press coverage and a degraded reputation among their customers, both of which can harm business.

### Challenge: Lacked Effective Security Testing Tool

Before deploying the Mu-4000, SonicWALL used manpower, homegrown test scripts, open-source tools, and other third-party test platforms to perform ad-hoc network security testing. Based on business metrics, this was not an effective approach. Before adopting the Mu-4000, SonicWALL's signature matching engine could detect and block less than 60% of known vulnerabilities.

### Benefit: Expedited Bug Remediation

After using the Mu-4000, SonicWALL now generates closer to 90% coverage against known vulnerabilities, much greater efficiency, and better reporting capabilities. Because the Mu-4000 provides a detailed remediation framework to streamline the interaction between QA and Engineering, SonicWALL finds it much easier for developers to reproduce and fix problems.

### Benefit: Quality Improvement Metric

SonicWALL also uses the Mu-4000 for one-touch regression analysis. Beyond offering them a time-based product quality improvement chart to show customers, this is a very efficient metric and ensures that new software builds do not inadvertently decrease the product's coverage.

SonicWALL knows IP-borne threats evolved over the last few years from script-kiddies to international organized crime. These groups are sophisticated and operate profitable businesses. It is very difficult to keep one step ahead but the Mu-4000 is an important tool to help focus its development team around this effort while ultimately building a higher-quality product.

# Mu-4000 Analyzer: Feature Highlights



The Mu-4000 analyzer automates the first rigorous, systematic and repeatable process for characterizing the reliability, availability, and security of networked products and

applications. The Mu-4000 is a self-contained, rack-mountable appliance. It is easily configured and managed via a web browser graphical user interface, and can also be controlled using any scripting language via a remote automation interface (via either a REST or WSDL API) for seamless integration with extant laboratory automation frameworks.

## Millions of variations on service traffic: Thorough and Precise Attack Surface Coverage

- Unique stateful protocol modeling engine interactively explores complex, stateful targets with millions of dynamically generated variations of protocol traffic tailored to the targets' exact capabilities;
- Adaptive analysis combines Mu-developed dynamic protocol fuzzing suites with a large number of transport and authentication options;
- Only solution to support dynamically constructed attack vectors for user-defined protocol extensions.

## Denial of Service Modules

- Create customizable DoS attacks and detail accidental or malicious impact on critical business services;
- Application level and protocol DoS attack capability with pre-defined templates for well-known attacks;
- Actionable results: Correlate traffic injection rate with faults and outages; Identify system recovery time and improve mitigation controls

## Shareable Templates: Knowledge Sharing and Best Practice Dissemination

- Helps disseminate scarce reliability, availability or security knowledge within organizations, ensuring consistent baselines and results;
- Basis for establishing common product deployment best practices across different departments;
- Enables reliable problem replication via sharing of analysis configurations.

## Response Time Charts: Quick Identification of Hot Spots

- Visually exposes reliability and availability issues, including response-time degradation, CPU utilization spikes – problems that lead to failures or implicit denial-of-service attacks;
- Identifies product weaknesses using an executive dashboard;
- Interactively hone in on hot spots for likely areas of downtime or poor quality.

## Automated Fault Isolation and Remediation Tools

- Advanced analysis engine pinpoints failures to a single unique attack vector when possible;
- Faults are ranked using the industry standard CVSS scoring methodology;
- Flexible user-defined fault definitions can use criteria like log output, system load, code coverage, etc.;
- Sophisticated, customizable reports include captured data as well as configuration templates.

## Automation Framework: Seamless Integration

- Fully automated service assurance process using a powerful customer-proven methodology;
- XML-based remote automation provides control of the Mu-4000 platform within any scripting language;
- Easy integration into existing analysis, laboratory automation frameworks and regression suites for both round-the-clock automated and on-demand service assurance.

## Protocol Solution Bundles

Mu Dynamics develops and offers the following solution bundles for various markets and customers:

- Admin
- IMS
- IPTV
- Storage
- VoIP
- DMZ
- Industrial Control
- Mail
- Routing

Visit our Protocol Page at [www.mudynamics.com/products/protocol.html](http://www.mudynamics.com/products/protocol.html) for briefs and updates.

*"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,"*

Paul Farley, Director of Network Intelligence & Security Engineering, Cox Communications

*"After deploying Mu Dynamics' Mu-4000 analyzer, understanding our customer's network security issues during highly complex network changes became a tractable problem."*

Vijay Nadkarni, VP of Engineering, Veraz

*"Mu's analyzer fills a critical void in the market today. Nothing previously available has been able to probe as effectively for exploitable flaws caused by layered protocols and their many interdependencies."*

Peter Fetterolf, Network Strategy Partners

*"As the editor and author of the SIP Torture Test, RFC-4475 and RFC-5118, I was particularly impressed with the Mu-4000 analyzer at SIPit SIPit 19, especially its dynamic ability to focus on meaningful tests that stressed elements far beyond basic parsing mechanics. I am suggesting new SIP analyses and tests for inclusion in Mu Dynamics' platform."*

Robert Sparks, SIPit Coordinator

*"The Mu-4000 is an analysis tool, perhaps the most robust analysis tool of its type that I ever have seen."*

Peter Stephenson, Contributing Editor, SC Magazine



THE AMERICAS | ASIA-PACIFIC | EMEA



web: [www.mudynamics.com](http://www.mudynamics.com) | email: [info@mudynamics.com](mailto:info@mudynamics.com)  
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA  
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317