

An underwater photograph showing a shark swimming towards the camera. In the upper left corner, the dark hull of a boat is visible. The water is clear and blue, with light filtering through from the surface.

 **Mu Security™**

Finding Hidden Dangers.

Service Providers

Businesses are Running on Fragile Networks

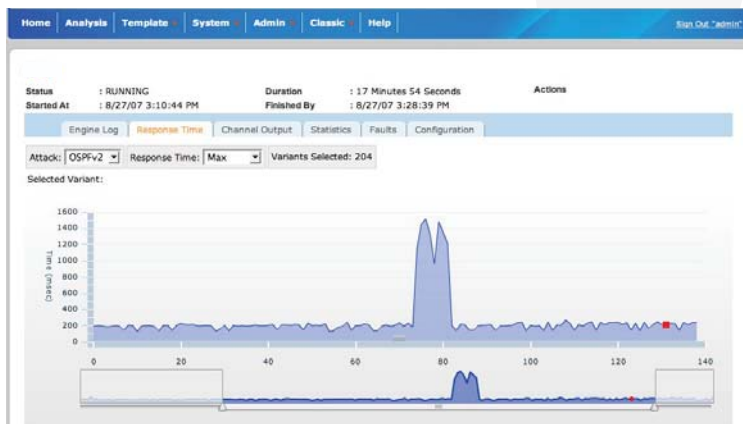
With networked products getting more complex, application-aware and inter-connected, network owners are increasingly concerned about the robustness and reliability of the networks they operate. Even though lots of money is being spent on perimeter security, systems are getting more vulnerable, not more secure. Needless to say, the losses from service disruptions, outages and network downtime are enormous for service providers.

Networked products, including perimeter security systems themselves (e.g., firewalls, IDS's), fail in production environments due to security or interoperability issues. These failures manifest themselves in the form of either outright system and/or application crashes or as response time spikes that affect service availability. The latter type of “soft” failures is more subtle and often goes undetected until a “hard” crash ultimately occurs. The root cause behind service-degrading “soft” faults has traditionally been extremely difficult for users to isolate, and for vendors to replicate and repair.

Proven Solution to Boost Service Availability

Mu Security's security analysis solution is deployed by top service providers worldwide. These users want to implement infrastructures that are resilient enough to sustain a reasonable level of quality of experience (QoE), even in the face of the most extreme traffic conditions. With Mu's solution, service providers and other users can detect and address even the most subtle vulnerabilities early on, and thus significantly reduce revenue loss and avoid customer churn caused by service quality issues.

Mu's solution takes a distinct approach of proactively assessing targets for application security issues including buffer overflows, resource exhaustion, CPU utilization spikes, etc. This solution provides users with an unbiased scientific characterization of a product's robustness before deployment.



"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 Security's solution is becoming indispensable to users who are methodically identifying the root causes of robustness shortcomings or deep-seated vulnerabilities in any IP-based product or service."

Mike Monticello
Security Analyst, Enterprise Management Associates

- Service outages?
- Network downtime?
- Customer churn?
- Losing to competition?

Case Study: A Major Cable Service Provider

A major U.S. cable triple-play multi service operator actively uses Mu's solution to improve security testing of their network equipments – and after only a year has achieved many business benefits.

Challenge: Robustness Issues Went Undetected

The security experts at this Cable Service Provider previously used homegrown scripts, and other open-source tools to test for security weaknesses. The problems they found with manual testing were relatively obvious; many subtle security flaws went undetected.

Benefit: 10x Test Coverage

With Mu's security analysis solution, the Cable Service Provider estimates achieving **TEN TIMES GREATER** test coverage compared to the manual approach. Using the Mu-4000 appliance, the Cable Service Provider quickly found flaws in a critical VoIP network element. These flaws would have resulted in serious denial-of-service conditions in the production network equating to opportunities for expensive network service outages.

Challenge: Scarce Security Knowledge in Silos

In the past, a small, specialized security incident response group did all security testing. This Service Provider used employ three staff security experts who spent 20–40% of their time on security testing. These are expensive resources and they are difficult to attract and retain. In contrast, the large product certification testing organization did not have sufficient security expertise to test for security. Without the Mu-4000, it would have been effectively impossible to add security metrics or process to this organization.

Benefit: Knowledge Dissemination and Best Practices

By handing off the “heavy lifting” of testing to a Mu-4000 system to automate, the security group now defines testing criteria and disseminates 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.

Benefit: Finding Bugs Early Saves Time and Money

The Cable operator also uses the Mu-4000 for new product evaluation and bake-off. By finding robustness issues as early as possible in product selection, it saves time and money in service deployment.

Software and Hardware Vendors

- Quality issues?
- Too many fire drills?
- Lack process?
- Need quality metrics?

Case Study: SonicWALL

SonicWALL, a leading firewall manufacturer, is using the Mu-4000 to improve their product's IDP signature capabilities to root out 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 appliance 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 devastate business.

Challenge: Lacked Effective Security Testing Tool

Before deploying the Mu-4000, SonicWALL used manpower, home-grown test scripts, open-source tools, and other third party test platforms to perform network security testing. It really had no effective solution. Prior to using the Mu-4000, the signature team achieved just below 60% coverage for known vulnerabilities.

Benefit: Expedited Bug Remediation

After using the Mu-4000, SonicWALL now generates closer to 90% coverage against vulnerabilities, much greater efficiency, and better reporting capabilities. Because the Mu-4000 provides detailed remediation tools that 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 testing. Beyond offering them a time-based product quality improvement chart to show customers, this is a very efficient metric and ensures new software does not 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 a profitable business. 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.

Vendors Are in a Bind

In the never-ending race to offer more features at a faster pace, vendors of networked products have lacked readily available 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 testing ever more important.

Production Bugs are Expensive to Fix

However, the fact remains: the cost of finding and fixing bugs in a production network is several orders of magnitude higher than fixing bugs before product 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.

NIST estimates that it is 30-50x cheaper to fix a bug in development than in the field.

Solution to Better Product Quality with Proven ROI

Mu's security analysis solution helps improve product quality without slowing down the product development process. The result is much fewer field fire drills and product delays caused by 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.

The Mu 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. Furthermore, the solution enables vendors to show quality commitment to their customers via a repeatable process and tangible metrics.

<input type="checkbox"/>		Enterprise Router HTTP Testbed: Enterprise Router Directly Connected Testbed Mu-4000 Interfaces: 1 Target: Enterprise Router
<input type="checkbox"/>		Enterprise Router OSPF Analysis Testbed: Enterprise Router Directly Connected Testbed Mu-4000 Interfaces: 1 Target: Enterprise Router

"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 Security 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 security for critical applications that require robust performance. 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."

Rod Couvrey, Vice President, Software Engineering
Redback Networks

Mu-4000 Security Analyzer: Feature Highlights



The Mu-4000 Security Analyzer delivers the first rigorous, systematic and repeatable process for characterizing the robustness 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 for seamless integration.

Sharable Templates: Knowledge Sharing and Best Practices

- Helps disseminate scarce security knowledge within organizations.
- Basis for establishing common security analysis best practices across different departments.
- Enables reliable problem replication via sharing of analysis configurations.

Response Time Chart: Quick Identification of Hot Spots

- Visually exposes quality and availability issues, including performance degradation, CPU utilization spikes, etc, which may lead to failures or denial-of-service attacks.
- Helps to identify product weaknesses using an executive dashboard.
- Interactively hones in on hot spots.

Dynamic Stateful Fuzzing: Thorough and Precise Attack Surface Coverage

- Unique stateful protocol fuzzing engine dynamically uncovers weaknesses of complex, stateful targets with attack vectors tailored to the targets' exact capabilities.
- Adaptive analysis combines Mu-developed protocol mutations with a large number of transport and authentication options.
- Only solution to support dynamically constructed attack vectors for user-defined protocol extensions.

Automated Fault Isolation and Remediation Tools

- Advanced analysis engine isolates failures to a single unique attack vector when possible.
- Flexible fault definition uses analyst-defined criteria like resource utilization, code coverage, etc.
- Sophisticated, customizable reports include captured data as well as configuration templates.

Automation Framework: Seamless Integration

- Fully automated security analysis process using the powerful "mutate-monitor-manage" methodology.
- XML-based remote automation provides access to the Mu-4000 platform from any scripting language.
- Easy integration into existing testbeds and regression suites for round-the-clock security analysis.

Protocol Solution Bundles

Mu Security has developed the following solution bundles for various markets and customers:

- Media
- DMZ
- Storage
- Admin
- Industrial Control
- Mail
- Routing

Visit our Protocol Page at www.musecurity.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 Security's Mu-4000 Security 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 Security 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 of the SIP Torture Test, RFC-4475, I was particularly impressed with the Mu-4000 Security Analyzer at 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 Security's 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.musecurity.com | email: info@musecurity.com
address: 686 W. Maude Ave., Suite 104, Sunnyvale, CA 94085, USA
phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317