

PRODUCT VENDOR
WHITEPAPER

**A PROACTIVE APPROACH
TO ELIMINATING COSTLY
FIELD FIRE DRILLS**

There's a tug of war between customers' demands for rapidly delivered, ultra-reliable IP products and competitive pressures on product vendors to sustain the pace of delivering innovative new products – on time and on budget. The challenges are compounded by the escalating complexity of real time IP services, including VoIP and IPTV, not to mention the transition to open networks from proprietary or single vendor systems.

With Mu Dynamics' service assurance solution and its built-in automation facilities, software and hardware product vendors can ensure that their IP-based products will meet customers' expectations for both quality and delivery schedule. Mu's solution methodically identifies and addresses quality issues early in the development life cycle, and provides vendors with an automation framework for easy integration into existing processes. The result is fewer field fire drills and product delays caused by quality issues. Vendors achieve significantly higher test coverage with reduced cost of product maintenance and support. Furthermore, Mu enables vendors to show quality commitment to their customers via a repeatable process and tangible metrics.



686 W. Maude Avenue, Suite #104
Sunnyvale, CA 94085
866-276-4640 toll-free
408-329-6330 international
408-329-6317 fax
www.mudynamics.com

welcome to the **BUG-FREE ZONE**



REAL WORLD IMPACT OF BAD SOFTWARE

Recent news headlines about product flaws contributing to network downtime and security incidents:

- [Unauthorized Web Servers Connected to IRS Network, SC Magazine](#)
- [Networks Riddled with Vulnerabilities, SC Magazine](#)
- [Oracle Issues 36 Patches, but Is Anyone Applying Them?, Computer World](#)
- [Cisco Patches 12 Vulnerabilities, SC Magazine](#)
- [Data Security Now 10 Percent of IT Operating Budgets, CSO Magazine](#)
- [Apple Fixes Security Bug with iPhone Update, InfoWorld](#)
- [TJ Maxx Parent Company Data Theft is Worst Ever, InformationWeek](#)

RECENT VULNERABILITIES DISCOVERED BY MUSEC

- [strongSwan IKEv2 Denial-of-Service Vulnerability, September 18, 2008](#)
- [Remote DoS in reSIPProcate, July 11, 2008](#)
- [Multiple Buffer Overflows in Asterisk, March 18, 2008](#)
- [Multiple Remote Arbitrary Execution Vulnerabilities in Mplayer, February 14, 2008](#)
- [Dibbler Remote Denial of Service Vulnerability, September 20, 2007](#)
- [Quagga bgpd Remote Denial of Service Vulnerability, September 18, 2007](#)
- [Helix DNA Server Heap Corruption Vulnerability, August 24, 2007](#)

The Growing Product Quality Problem

As IP-based applications move to open standards and are increasingly more inter-connected, they have dramatically more risks due to the growing complexity. These applications are thus more prone to quality issues that negatively affect product vendors' revenue and damage customers' confidence.

Software with weaknesses or interoperability issues costs tens of billions of dollars per year in the U.S. alone, and represents just less than one percent of the nation's GDP, according to the National Institute of Standards (NIST).¹ Many factors contribute to software quality issues, including vendors' aggressive marketing strategies, their limited liability, and diminishing returns for testing and debugging, especially in light of an industry-wide innovation arms race.

Software users – network operators, corporations, educational institutions, government agencies, and others – bear the brunt of the software quality costs, in the form of software patching and other risk mitigation activities. Microsoft and Wipro determined a 1000-person company's average annual cost of patching Windows servers alone is \$1.6 million – and that's using automated patch tools and best practices.²

Software developers simply can't scale existing manual processes, many of which were developed 10 or more years ago. Spending more to avoid field fire drills or boosting QA spend in the form of testing is often considered only after a customer incident. Inadequate testing processes, tools and methods used by product vendors are often the root cause for:

- Lost revenue due to poor product quality
- Higher software development costs
- Increased time to market due to inefficient testing
- Diminished customer satisfaction

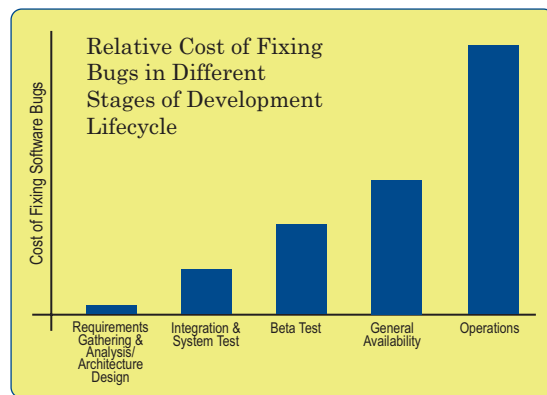
For the customer, downtime costs vary greatly by industry and company size.

- **Network Operators.** VoIP or IPTV downtime directly translates to lost revenue because of service level agreement (SLA) penalties and increased customer churn. For a typical service provider, outages cost more than \$100,000 per hour for business customers, according to studies by Light Reading and NSP Partners.³
- **Industrial Control.** Users are highly dependent on high-quality IP services, including networks and electric power. Power outages and network quality problems cost more than \$20,000 per year per establishment, according to the Consortium for Electric Infrastructure.⁴

Closing the Loop on Quality

Vendors of IP products strive to develop and deliver high quality products on time and on budget, but closing the loop on quality is challenging, because of multiple dynamics:

- **Compressed development times and skyrocketing complexity increase product flaws.** Product flaws and vulnerabilities that cause service availability, reliability or security issues creep into product development and upgrades because of incomplete or inadequate quality assurance. The use of open source software and distributed development exacerbates the quality problem and makes the needs for system-level testing and analysis all the more urgent. Finding and fixing interoperability, robustness or security bugs as early as possible in the software development lifecycle (SDLC) has a clear advantage: NIST estimates there is more than 10x cost saving to fix a bug in development than in the field.



¹ The Economic Impacts of Inadequate Infrastructure for Software Testing, National Institute of Standards and Technology, May 2002.

² Total Cost of Security Patch Management, Wipro and Microsoft. http://download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf

³ Estimates based on an ROI model developed by Network Strategy Partners, LLC.

⁴ The Cost of Power Disturbances to Industrial and Digital Economy Companies, A study by Primem (Now owned by IDC), funded by CEIDS, June 2001.

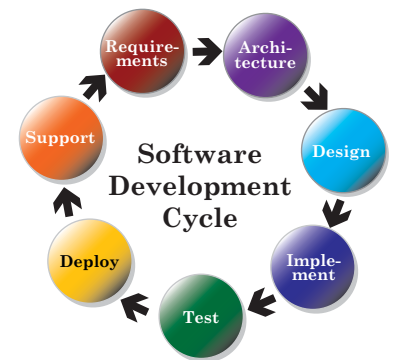


- **Greater reliance on IP and open standards.** Every networked product, service, and application is moving to an IP-based infrastructure. Formerly isolated control or proprietary products in homogeneous networks are migrating to heterogeneous systems. IP infrastructures are inherently complex and diverse, and thus fragile. Open, standardized communications protocols are exposed to a wide variety of potential security attacks and weaknesses.
- **Migration towards IPv6.** Many government agencies, industrial control operators and large enterprises are migrating to IPv6 for its expanded capacity and other improvements over IPv4. The move is not without obstacles. The complexity of IPv6 deployments, compounded with the immaturity of IPv6 deployments, means systems are more fragile and vulnerable, which creates new opportunities for network downtime and service disruptions. Repeating the mistakes of complex IPv4 deployments again with IPv6 is a distinct possibility.
- **Next-gen network (NGN) market opportunities.** Organizations are rapidly adopting VoIP, streaming media, mobile applications and other new IP-based applications in an effort to maximize productivity and save money. The relative youth of VoIP and the use of new protocols like SIP create complexity for VoIP hardware and software developers. Plus, customers expect their VoIP system will meet or exceed the prior industry-standard benchmark for service quality, availability and security. As high-quality IP video emerges, vendors are challenged by the overwhelming challenges of assuring multi-vendor interoperability as well as the reliability and security of their own products.



Meeting the Challenges of Product Reliability, Availability, and Security

Mu Dynamics provides an award-winning service assurance solution for improving the service availability of IP-based products. Product vendors leverage Mu's solution as part of their SLDC best practices to verify that their products will be reliable, available and secure once deployed to customers.



Product vendors use Mu to:

- **Deliver high-quality products on budget and on time.** Product vendors depend on Mu for an easy-to-deploy solution that helps product development and QA teams automate existing/new testing suites and reduce reliance on manual, home-grown test scripts. With Mu, product vendors automate the discovery and elimination of many quality issues. If left unchecked, these software weaknesses result in outright system crashes, DoS exposures, and more subtle issues such as response-time latency and CPU utilization spikes, before the product ships.

Developers leverage Mu's automation capabilities across the SDLC – and by all parties in distributed development team. During design and development phases, developers use Mu to exercise code for robustness, so that flaws are fixed earlier in the process. QA teams use Mu to integrate methodical negative testing to improve productivity. With Mu's automated testing, developers gain key insights and actionable metrics that they use to anticipate latent service availability issues.

- **Expedite customer problem resolution.** Vendors use Mu to isolate problem areas and analyze the root cause of a problem before the product is commercially available. Accelerated problem resolution becomes more urgent after the product is released, and vendors use Mu to vet the effectiveness of software patches and configuration changes to resolve issues with minimal customer impact. Mu's detailed reports, interactive charts and packet captures help developers expedite problem resolution across the SDLC. Mu's interactive Response Time Charts visually spotlight and document spikes in the network response time.



Figure 1. An example of Mu's Response Time Chart

Development teams often lack the visibility into the interactions of the many layers of IP protocols to proactively analyze service availability and product reliability. With Mu's Shareable Analysis Templates acting as XML-based knowledge macros, development teams can quickly build and disseminate analysis templates across a distributed development team to establish a set of repeatable best practices that can reduce the instances of flaws that can later impact service availability and security.

"Mu's approach is to proactively address their customer's widespread need for better network and product service assurance including the clear identification of reliability issues, faults and other attack-surface weaknesses."

Chris Christiansen
 VP, Security Products &
 Services
 IDC



- Smooth the migration to IPv6.** Mu offers a comprehensive solution to help product vendors streamline IPv6 service assurance. Since IPv6 is much more complex than IPv4, many product vendors have not yet mastered best practices in programming and deployment in native and transitional environments. Mu helps organizations methodically find and eliminate potential weak spots in new IPv6 implementations or deployments. Product vendors can use Mu to identify and remove both IPv4 and IPv6 weaknesses to ensure reliability, availability, and security.

Detecting distributed attacks and new spoofing techniques over IPv6 is much harder because of the larger address space of IPv6. Mu provides rapid identification and detailed auditing of IPv6 weaknesses before they cause costly downtime. Mu automates finding structural as well as semantic flaws across IPv6 implementations in hosts and routers, which may result from IPv6's optional headers, which are more complex than in IPv4.

The Proactive Service Assurance Solution from Mu

The Mu Service Analyzer can be used to systematically identify weaknesses in any IP-based application and network product, including the following:

- Multi-layer Security Products:** Unified threat management (UTM) is the first line of security defense for many end customers. However, with the integration of many security applications, UTM vendors are often challenged to find the unintended vulnerabilities that lie dormant in their own code base because of the near infinite number of settings in combination of UTM applications: firewall, Web filtering, virus screening, spam filtering, intrusion prevention, and VPN.

With Mu, security vendors can efficiently test millions of variations on service traffic so that the entire analysis process is structured and repeatable. Vendors can ensure that their UTM products are thoroughly vetted for software weaknesses that could impact service before the product is deployed in a customer's production network.

- Network Infrastructure and Storage:** Next-generation network and storage infrastructure has more functionality – routing, switching, security, quality of service, virtualization, and more – and at higher speeds than ever before. As product vendors keep up with enterprises' and service providers' need for integrated functionality and higher capacities, it is paramount to ensure that vulnerabilities and weaknesses do not creep in.

Vendors depend on Mu to assist in their development environment and test implementations of key protocols such as TCP and BGP4. Mu helps the vendor harden the implementation of numerous protocol suites for a wide variety of product development efforts. Benefits include a noticeable decrease in customer reported new vulnerabilities on both product upgrades and newly released products.

- VoIP Infrastructure:** Ensuring the security and reliability of VoIP products can be daunting. A VoIP system depends on many inter-related components, and each component is in itself a complex, standards-based hardware or software system. As the network complexity exponentially increases, implementation mistakes and interoperability issues are magnified.

Mu helps VoIP vendors identify sources of service quality problems in their products before they impact the customer experience. Mu provides thorough attack surface coverage of the protocol implementation across a VoIP system, including SIP and underlying mechanisms such as HTTP and SMTP/MIME. Mu helps vendors overcome robustness challenges that arise because of SIP's large number of semi-interoperable implementations and many extensions.

- IPTV and Real-time Media:** Next-generation IP video networks are complex systems comprised of many different hardware and software products making them difficult to design and deploy. The challenge is compounded by their heavy dependence on a relatively new protocol - Real Time Streaming Protocol (RTSP). RTSP expertise is in short industry supply yet is extremely valuable as the protocol helps deliver content to millions of customers over broadband networks.

Mu can help product vendors discover IPTV service availability weaknesses that result from protocol vulnerabilities. Developers use Mu to test their IPTV gear, including multimedia terminal adapters, CMTS, set-top boxes, home gateways, edge and core routers, L2 switches and DSLAMs across a broad array of IPTV protocols, including IGMP, RTSP, SIP, H.248, MGCP, PIM, SNMP, IPv6 and more.



- **Mobile wireless infrastructure:** Mobile operators today generate more than \$2.1 trillion in worldwide service revenue for more than 9 trillion voice minutes and 1.8 billion mobile subscribers. These operators are increasingly deploying IP-savvy backhaul and provisioning products to grow their business opportunities with broadband-speed data and video access. All of the services require complex IP equipments and applications for high quality mobile voice and data services.

Mu helps mobile infrastructure vendors ensure their products contain no weaknesses that could result in downtime or degraded service quality. The Mu solution provides valuable benchmark for new and existing revenue-critical services including email, music, PDA bundle and other portable applications.



“Ditech Networks’ voice quality solutions have a strong reputation for carrier-grade reliability, and Mu’s stateful solution ensures the rapid removal of VoIP weaknesses during product development to ensure the highest quality solution for our customers. As Ditech’s Voice Quality products gain more features and VoIP service complexity increases, Mu’s product will help our development team proactively isolate and eliminate issues that could cause downtime for our customers during deployment and operation.”

Conne Skidanenko
Sr. Director of Engineering
Ditech Networks

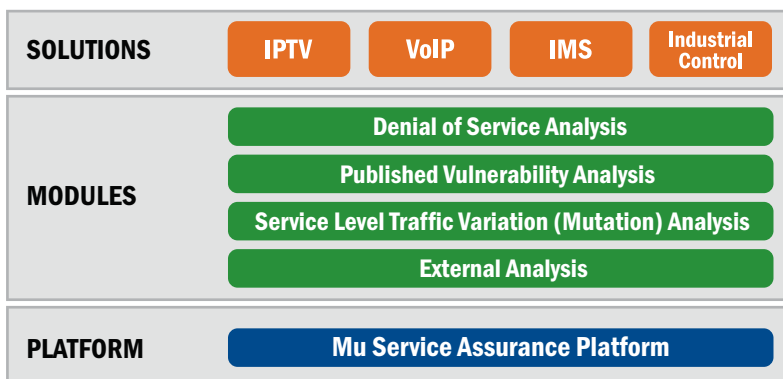


“Our customers have built highly available, reliable and secure networks using Force10 products, but we are always searching for newer ways to test our products. The Mu Dynamics solution effectively probes for not-so-obvious vulnerabilities in protocol implementation in a unique way and has become an important part of our testing process, enabling us to build more stable, secure and reliable routing, switching and security products.”

Tushar Patel
VP of Engineering for Test
and Quality Assurance
Force10 Networks

Core Analysis Modules

The Mu service assurance solution offers four core analysis modules to help product vendors improve quality and dramatically reduce field fire drills.



- **Denial of Service (DoS) Analysis.** Mu’s DoS Analysis module helps product vendors simulate a wide variety of known and customized distributed DoS attacks, worms, botnets and amplification attacks in a controlled environment. XML templates make it easy to build realistic DoS attack simulations for IP-based applications and services. Mu automatically gathers detailed data during the DoS simulation, and provides metrics on outages as well as recovery time.
- **Published Vulnerability Analysis (PVA).** Product vendors use the Mu PVA module to demonstrate for themselves whether a given signature in a networked product device is actually effective at detecting or blocking specific undesirable traffic. Vendors can become aware of the existence of any traffic that is not blocked by the product or service under analysis, such as a zero-day attack. The PVA module applies repeatable metrics to verify the proper operation of any inline signature-based network product, including Intrusion Prevention Systems (IPS), content-aware security gateways, deep-inspection firewalls and Unified Threat Management (UTM) systems.
- **Service-level Traffic Variation Analysis (a.k.a. Mutation Analysis).** Service-level traffic variations use protocol mutations designed to undermine the reliability and availability of an application, product or service and to expose underlying weaknesses. Mu generates millions of service-level traffic variations in a wide range of VoIP, IPTV, IMS and other widely-used application protocols. Mu’s dynamic service level traffic mutations allow identification of previously unknown service weaknesses and vulnerabilities in a target application or device.
- **External Analysis.** The Mu platform separates the notion of service modeling with the service monitoring. While Mu provides numerous ways of generating traffic variations, there are thousands of existing scripts and tools (internally developed, free, open source or commercial) in which a customer might have an investment. With External Analysis, the Mu solution is able to leverage its significant automation infrastructure to bear to improve the usability of the tools, thereby vastly improving this aspect of the development and QA staff.



“After deploying Mu's Mu-4000 Analyzer, understanding our customer's network availability and security issues during highly complex network changes became a tractable problem. We have been pleased with the commitment and support provided to us by the Mu Dynamics team and with the system's ability to help us proactively identify complex security issues in widely varying VoIP and underlying SIP configurations.”

Vijay Nadkarni
VP of Engineering
Veraz Network



"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 service assurance for critical applications that require robust performance.”

Rod Couvrey
Vice President of Software Engineering
Redback Networks

Eliminating Fire Drills with Mu: Customer Use Cases

Mu helps product vendors create and sustain more reliable, available and secure products through proactive service assurance. Vendors leverage Mu's automation throughout their product development lifecycles.

The following real-life examples and case studies speak volumes of the value of Mu's solution.

Mu to the Rescue

Problem Discovered Using Mu	Impact if problem Deployed in Production Network	Mu Solution(s) used to Uncover Root Cause
FTP application filter dropped sessions erroneously	Interruption in legitimate customer traffic, loss of application connectivity	Mu Service Level Traffic Variations/Protocol Mutation module, FTP option
Softswitch SIP traffic was bleeding over to billing system, crippling billing server	Downtime in billing applications cost \$\$ millions in lost transaction data and often disrupt customer calls	VoIP bundle including SIP in Mu's Service Level Traffic Variations/Protocol Mutation module
IPv6 software bug discovered in leading core router vendor, when facing service traffic it caused a broadcast attack	IPv6 weakness would bring down entire cluster of core router, loss of all core and edge IP services depending on that router connectivity	IPv6 Mu Service Level Traffic Variations/Protocol Mutation module
DNS-based DoS VoIP attack weakness in operator network, VoIP domain resolution wiped out with no connectivity	Complete loss of all customer VoIP services for more than 3 hours with hourly cost more than \$150,000 per hour	Mu DoS module and DNS using built in and customizable Mu-4000 SIP service monitoring and instrumentation
Incomplete and outdated vulnerability signatures, reliance on exploits instead of underlying vulnerability information caused weakness in deployed network products	Malicious exploit of the security products, core network and IP applications	Deploying Mu's PVA capabilities to automatically detect and fix a far greater range of published vulnerabilities with fewer IT resources in less time Significant competitive and time-to-market advantages as well as major cost savings for the vendor's product software development lifecycle (SDLC)
SSH bug rendered a major Unix-based server platform completely unusable and corrupted the hard drive	Had the bug not been found in time, the rollout of a new, vulnerable version of Unix could have cause a major and costly outage of all platform-enabled services	Methodical and consistent usage of the Mu SLTV module throughout the deployment lifecycle
DHCP weakness in SOHO firewalls in wide deployment prevents IP connectivity for customers	Had this bug been widely exploited or triggered by a worm, large numbers of customers would have lost IP connectivity from their ISP, and the ISP would have had to recall all devices as there was no field remedy	Methodical and consistent usage of the Mu SLTV module throughout the deployment lifecycle
Application layer DoS weakness in VoIP softswitch causes loss of service and system crash	A SIP DoS attack brought down a core SIP softswitch, and the system was unable to recover without manual intervention. Complete loss of service.	VoIP bundle including SIP in Mu's Service Level Traffic Variations/Protocol Mutation module



"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



"Our customers require high-performance security products to be highly resistant to either inadvertent or malicious Denial of Service (DoS) weaknesses. Mu helps our product development teams to ensure that customer's services using Juniper-based infrastructure are fast, reliable and secure – ultimately reducing costly application downtime."

Michael Frendo
Senior Vice President,
High-End Security Systems
Juniper Networks, Inc.



"Most IT vendors perform security analysis and point testing on a hit-and-miss basis. Decru has invested in a broad range of internal testing, third party lab reviews, and government certifications to ensure the highest level of security. The Mu analyzer provides a powerful tool to automate and expand our security testing procedures, which in turn helps us identify issues early in the development lifecycle."

Kevin Brown
Vice President of Marketing
Network Appliance/Decru.

F5 Enhances Robustness, Resiliency and Reliability of Application Delivery Products

F5 uses Mu Dynamics' Service Assurance platform to discover, document and eliminate potential security and robustness vulnerabilities for its BIG-IP and WANJet products. F5 uses Mu to automate vulnerability auditing and remediation processes throughout its product development lifecycle. As a result, F5 is ensuring its customers operate the most robust, high performance and secure systems built to remain resistant to hacker attacks and network downtime.

F5 bolsters its product design, development and quality assurance lifecycles using Mu to meet key customer security metrics based on a broad and deep analysis of each product's attack surface. For example, SIP analysis ensures optimal VoIP application performance, as well as security and robustness readiness throughout F5's comprehensive product line. By applying a rich suite of user-defined protocols over IPv4 and IPv6 transport, measurement and testing is automated throughout F5's product design, development and deployment phases, including product upgrades and patches.

Juniper Networks Enhances Proactive Security using Mu Dynamics

Juniper Networks relies on Mu Dynamics' Service Assurance platform to bolster its J-Security and Security Assurance development team efforts. By integrating Mu into Juniper's established product development processes, Juniper enhances the security analysis lifecycle of its design and development efforts for products, including Firewall/VPN and IDP. As a result, Juniper can proactively identify, isolate and quickly update its products' ability to defend against network- and application-level attacks before they inflict any damage, minimizing the potential downtime and costs associated with these attacks.

Avishai Avivi, senior director, DPI Technologies at Juniper Networks, said that to ensure a high level of ongoing security with both new products and updates to existing platforms, Juniper has added the Mu-4000 Service Analyzer to its pre-release testing efforts. It is using the analyzer as an automated regression test bed for products across various groups within the company, including the Service Layer Technologies Group that handles firewalls, intrusion detection, WAN accelerators and more; the Integrated Products Group that supports the routers; and the Ethernet Products Group. "Using the Mu box, we can run millions of tests and run them quickly, accurately and repeatedly," Avivi said. "Tests have to be repeatable and there's nothing that can run a test like a machine. A machine doesn't get tired or care that it is 2 a.m. and your test just crashed. It just restarts the test automatically. There is some real cost savings there."

NetApp Enhances Secure Development and Deployment of Decru Storage Security Appliances

Decru, a Network Appliance company, uses Mu Dynamics' Service Assurance platform to enhance its investment in secure development processes and ensure the highest level of security for its storage security appliances. Decru uses Mu to automate and extend its existing security analysis procedures, which in turn helps Decru's customers deploy best-in-class privacy controls for sensitive data.

"Most IT vendors perform security analysis and point testing on a hit-and-miss basis," said Kevin Brown, Vice President of Marketing at Decru. "Decru has invested in a broad range of internal testing, third party lab reviews, and government certifications to ensure the highest level of security. The Mu Security analyzer provides a powerful tool to automate and expand our security testing procedures, which in turn helps us identify issues early in the development lifecycle."

SEL Automates Security Analysis for its Product Family

Schweitzer Engineering Laboratories (SEL) uses Mu Dynamics' Service Assurance platform to discover, document, and eliminate potential security and robustness vulnerabilities for its digital protective relays and automation equipment. SEL chose Mu to expand vulnerability auditing and remediation processes throughout its product SDLC. As a result, SEL continues to ensure it upholds the quality and security customers expect, and as the technology advances, so too does SEL product development. SEL customers also benefit from robust, high-performance systems built and tested to remain resistant to malformed packets, hacker attacks, and system downtime.

"Our customers depend on SEL products to maintain the highest levels of system availability and robustness," said Rhett Smith, Security Products Development Manager at SEL. "By using Mu's Service Analyzer in our SDLC, we ensure SEL products are security-hardened before they ship to our customers."



"Mu Dynamics helps Starent Networks ensure we are delivering a more robust product, allowing us to add features with more confidence, so that our operator customers can reliably count on our product suite"

Andy Capener
VP of Marketing
Starent Networks

Starent Taps Mu to Strengthen Quality of Real-time Multimedia Applications

Maintaining real-time application reliability and security, while constantly providing new features, is a tall order. To address the full spectrum of quality challenges faced throughout the SDLC, Starent Networks turned to the Mu analysis platform.

The Mu solution greatly reduced Starent's rate of field fire drills and product delays caused by avoidable quality issues without slowing down the product development process. Moreover, Mu has helped Starent Networks identify product issues at earlier SDLC stages. This reduces rework, lowers the cost of fixing bugs, and accelerates time to market. Most importantly, Mu's proactive service assurance solution allows Starent Networks' development teams to systematically address even the most deep-seated reliability issues before its operator customer applications are deployed in production environments. Consequently, the company helps its operator customers deliver networks, services and applications that are resilient enough to sustain an acceptable quality of experience, even in the face of the most challenging real-world scenarios.

About Mu Dynamics

Mu Dynamics proactively eliminates the high cost of service, application and network downtime. Mu's solution automates a systematic and repeatable process that identifies hard-to-detect sources of potential downtime within IP services, applications and underlying networks. The award-winning Mu solution is deployed at more than 100 locations, primarily at leading global service providers, cable operators and network product vendors. Headquartered in Sunnyvale, California, Mu is backed by leading venture capital firms that include Accel Partners, Benchmark Capital, DAG Ventures and Focus Ventures. <http://www.mudynamics.com>



web: www.mudynamics.com | email: 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