

WHITEPAPER

The Business Case and Return on Investment for Deploying the Mu-4000 Security Analysis Platform

This new Network Strategy Partners (NSP) study highlights the business case for reducing costs and minimizing business risks by using the Mu-4000 analyzer provided by Mu Dynamics, Inc. NSP interviewed numerous Mu customers to help users calculate the Return-on-Investment (ROI) in a variety of common network scenarios. Increasing financial benefits underlying the ROI analysis, including optimizing a user's network operation Total Cost of Ownership (TCO), are derived from the fact that:

- Network outages in service provider, critical infrastructure, and enterprise networks result in high costs: The Mu-4000 improves service availability through robustness analysis of network elements.
- Finding and fixing bugs as early as possible in both enterprise and product vendor development lifecycles is significantly less expensive than in a production network: The Mu-4000 helps both service providers and network equipment manufacturers find bugs before products and services are deployed in production.

To help the reader establish the business case and ROI for the purchase of a Mu-4000, this paper includes ROI modeling calculations and results, as well as other real-life examples from Mu Dynamics' customers realizing these benefits. The study answers the following questions:

- Why should network services and products be tested for robustness?
- What is the ROI for Mu's analysis solution?
- What impact will security analysis have on Network Operation TCO?
- What organizations can benefit from the Mu-4000?
- What are service provider and product vendor use cases?



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



Business Drivers for Security Analysis

IP Convergence

Networks around the globe are converging to IP transport. Service providers are migrating all voice, video, and data services to converged IP-based networks. Enterprises worldwide are running converged corporate intranets and private voice over IP (VoIP) networks, and critical infrastructure providers are evolving toward running traditional IP protocols for industrial control systems used to manage critical ModBus or SCADA-based resources for the nation's utility and manufacturing infrastructures.

Increasing Complexity

In the never-ending race of offering more features at a faster pace, networked products and services are getting more complex, open, application-aware and inter-connected, making it a real challenge to ensure robustness and reliability. Accelerated use of open-source software and distributed development efforts further exacerbates the problem, making system robustness testing ever more important.

Complex, Fragile and Ultimately Vulnerable Networks Lead to High Risk Exposure, Higher Cost of Ownership

With the increasing complexity, it is more likely for unforeseen outages, downtimes, disruptions or even malicious exploits to occur in networked business systems. These robustness issues are not acceptable in mission-critical communication networks. They have a negative impact on service providers' service availability, customer quality of experience (QoE), the firm's competitiveness and reputation. In other words, network vulnerabilities cause businesses to have high risk exposures in revenue loss, customer churn, as well as penalties and legal entanglements from unmet service level agreements (SLAs).

Reactive Defense Not Working, Vulnerabilities Increasing

In an attempt to address these problems, businesses have been spending a large amount of money on equipments and labor directed to layered defenses in the network, such as firewalls, UTMs, etc. However, vulnerability monitoring organizations, such as CERT, report that highly and extremely critical advisories continue on a clear upward trend despite increased spending on layered defense security products. Clearly, the reactive approach to security does not work. A more proactive approach is needed.

Existing System Testing Tools Are Insufficient

Many organizations, such as service providers and software/hardware vendors, want to be proactive about improving service availability and product quality, but have lacked effective tools to help them.

Existing system testing tools have a few major limitations:

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

As a result, the goal of ensuring robustness, availability, and security of IP-based systems has been very difficult to achieve. Failure to achieve these business operational benchmarks also contributes heavily to increased network operation costs and lower return on network asset investments. .

Benefits of Security Analysis

To address these business problems, Mu Dynamics offers a unique system robustness testing solution to help proactively expose product robustness issues before they become critical. Mu's solution provides more depth, agility and breadth than traditional testing tools, delivering a significant, tangible ROI while optimizing network operation TCO.

Mu's Security Analysis Solution

The Mu-4000 takes a distinct approach of proactively analyzing IP networks for robustness issues including buffer overflow, resource exhaustion, performance degradation, etc. With Mu's solution, service providers and other users detect and address even the most subtle vulnerabilities early on, and thus significantly reduce the risk of revenue loss and customer churn caused by service quality problems.

The Mu-4000 security analysis platform methodically roots out robustness issues that result in downtime or unavailable networked applications caused by the following:

- intentional hacker activities (targeting deep-seated product vulnerabilities arising from software bugs, such as protocol implementation flaws);
- unintentional protocol anomalies that occur naturally (these are amplified from wide use of open-source software and outsourcing, and cause downtime by accidentally triggering the same bugs that the hackers seek);
- unexpected network configurations or device interaction, which can be avoided through proactive testing.

Automation Platform for Negative Protocol Testing

Mu's security analysis solution focuses on addressing protocol implementation weaknesses because 1) they are the root cause of the majority of network vulnerabilities, and 2) failures in protocol implementations can have disastrous consequences, putting businesses at risk of information leak, data loss, service disruptions, etc.

Protocol implementations are critical to the function of a larger system, because they enable communication among networked systems. However, protocol implementations are vulnerable due to reasons including:

- they have less control over their inputs (for example, a potentially buggy implementation of the same protocol could send packets across a network that re-orders, drops, mangles, and otherwise abuses those packets, and does damage to the local system);
- they are often deeply embedded within the system at a low level, which makes their bugs very difficult to isolate and fix.

The Mu-4000's is uniquely able root out robustness issues in protocol implementations thoroughly and accurately via its negative testing automation platform. The Mu-4000 automatically generates test cases that scientifically probe the nearly infinite space of invalid inputs. These targeted test cases (simulated attacks) can be run in a finite amount of time and still cover the code in all the necessary states, establishing that the implementation is able to handle a diversity of invalid inputs and still maintain the desired level of service and quality.

Wide Applicability of Security Analysis

In order to ensure networks are robust and secure, security analysis is adopted by a wide ranger of organizations:

- Users of networked products, as part of procurement, acceptance testing and change control processes:
 - Service providers like Cox Communications
 - Critical infrastructure vendors and asset owners like ABB and Honeywell
 - Enterprises including a number of government agencies
- Vendors of networked software or hardware products, as part of the software development lifecycle (SDLC) including F5, RedBack and SonicWall.

High Costs of Network Downtime

As network services converge to IP, service availability of the IP network is critical. Downtime and security breaches — whether as a result of network attacks, software errors, or configuration errors — often result in high costs. The cost of downtime is highly variable based on the business and applications. Estimates of downtime costs for various industries and applications¹ are presented in Table 1.

¹ See "Storage Virtualization and the full impact of Storage Disruptions: Relief and ROI", *Computer Technology Review*, February 2002, Volume XXII Number 2.

Industry	Application	Average Cost/ Hour of Downtime
Transportation	Airline reservations	\$ 89,500
Retail	Catalog sales	\$ 90,000
Media	Pay-per-view	\$ 1,150,000
Financial	Credit card sales	\$ 2,600,000
Financial	Brokerage operations	\$ 6,500,000

Table 1
Downtime Cost Estimates in Varied Business Markets

Impact on Service Providers

Downtime in service provider networks usually results in lost revenue due to SLA penalties and increased customer churn – poor ROI and TCO metrics follow. NSP Partners research found² both residential and business hourly revenue loss metrics for service provider network outages in metro areas where 100,000 residential customers and 2,000 business customers are affected by an outage. In these service areas, residential losses are estimated to be more than \$8,300 per hour and business losses almost \$6,950 per hour.

	Residential	Business
Number of Customers	100,000	2,000
Average Revenue per Customer	\$60	\$2500
Estimated Hourly Lost Revenue in an Outage	\$8333	\$6944

Table 2
Estimates for Service Provider Hourly Lost Revenue from Business and Residential Network Outages

While revenue loss is problematic, the potentially more serious problem (especially in markets where there are competitive offerings) is customer churn due from poor service. Table 3 presents a scenario for a metro area with 100,000 customers, an increased churn rate of 5% due to dissatisfaction with network service availability, and an average cost of churn of \$400 per subscriber based on time-based replacement costs. In this scenario the average cost of churn for this small metro area would be \$2,000,000 per year. Clearly, network reliability and availability is a critical business requirement for government agency enterprises and service providers.

	Churn Parameters
Number of Residential Subscribers	100,000
Increase in Churn Rate	5%
Cost of Churn per Subscriber	\$400
Total Cost of Churn per Year	\$2,000,000

Table 3
Service Providers Costs of Increased Churn due to Network Outages

A number of government agencies face similar issues with falling ROI on expensive networking investments if they fail to meet Service-Level-Agreements (SLAs) to which they have committed themselves. While they may not worry about churn, decreased network uptime contributes heavily to lower staff efficiencies.

Impact on Critical Infrastructure Providers

For critical infrastructure providers, the ramifications and cost of system downtime is more extreme. In June 2001, the Consortium for Electric Infrastructure to support a Digital Society (CEIDS) commissioned a study³ with Primen to obtain an estimate of the direct costs of power disturbances to U.S. companies. The costs include both outages and Power Quality (PQ) disturbances.

² These estimates are based on an ROI model developed by Network Strategy Partners, LLC.

³ *The Cost of Power Disturbances to Industrial and Digital Economy Companies*, A study by Primen (Now owned by IDC) funded by CEIDS, June 2001.

Critical infrastructure businesses account for more than 2 million business establishments in the U.S., which is roughly 17% of all U.S. establishments. Combined, they account for 40% of the gross domestic product and are highly dependent on high-quality services including networks and electric power. Power outages and network quality problems can cost more than \$20,000 per year per establishment for each of these establishments. EPRI notes that the total costs due to poor services including power and network failure to the U.S. economy – noted in Figure 1 - is a staggering \$119 to \$188 *billion* per year.

Based on NSP study findings the safety and robustness of networked critical infrastructure products in electric power utilities is of paramount importance. The fixed cost of proactively analyzing, testing and hardening the process and control-based systems used by the electric power utilities is relatively small compared the overall costs of power outages and PQ disturbances.

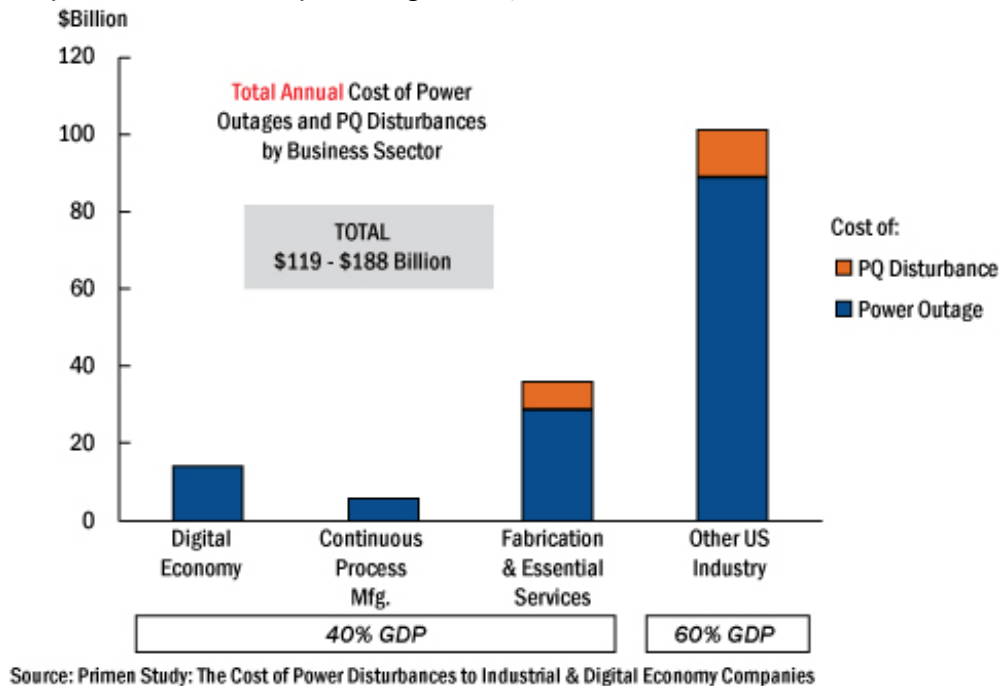


Figure 1
Total Annual Cost of Power Outages and PQ Disturbances by Business Sector

Mu-4000: ROI for Service Providers and their Suppliers

So far, this study demonstrates significant financial benefits to bolstering ROI and minimizing TCO through use of the Mu-4000 by service providers, enterprises, and critical infrastructure providers to improve network availability. This section of the paper details savings achieved by improving product quality and finding bugs in products before production deployment. Benefits here address both service providers and vendors of software and hardware products. The following sections detail the specific results of ROI models.

Cost Benefits of Early Bug Detection for Network Equipment Manufacturers

A well-known principle of software engineering details it is far less expensive to fix bugs earlier rather than later in the development lifecycle. A NIST research report⁴ provides a 10x savings metric through a study of these costs. Some of the report findings are used in this ROI model.

⁴ *The Economic Impacts of Inadequate Infrastructure for Software Testing*, NIST, May 2002.

Stages of the software development lifecycle are:

1. Requirements Gathering and Analysis / Architecture Design
2. Coding / Unit Test
3. Integration and System Test
4. Beta Test
5. General Availability

The relative cost of fixing bugs in various stages of the development lifecycle is presented in the NIST report and reproduced in Table 1. This table represents the cost of fixing bugs in each stage of development relative to the first stage of requirements and architecture. For example a bug found in the coding and unit test stage is five times more expensive to fix than one found in the architecture design stage. Similarly, when a bug is found in a production network after the software has been released it is 30 times more expensive to fix than a bug found in the architecture and design stage.

Requirements Gathering and Analysis / Architecture Design	Coding / Unit Test	Integration and System Test	Beta Test	General Availability
1X	5X	10X	15X	30X

Table 1
Relative Cost of Fixing Bugs in Different Stages of the Development Lifecycle

The distribution of bugs also is presented in the NIST report and depicted in Table 2. This table shows the typical distribution of finding and fixing bugs in each stage phase of the development lifecycle. Therefore, if bugs are found and repaired earlier in the cycle through negative testing, then engineering development costs are significantly reduced.

Requirements Gathering and Analysis / Architecture Design	Coding / Unit Test	Integration and System Test	Beta Test	General Availability
15%	20%	40%	15%	10%

Table 2
Typical Distribution of Bugs in Software Development Lifecycle

The Mu-4000 helps reduce the costs associated with the software development lifecycle (SDLC) including the overall cost of software bugs and improves product quality by allowing development organizations to detect and repair defects earlier in the process. In order to quantify these benefits, an ROI model follows that uses NIST assumptions presented in Table 1, Table 2 and Table 3.

	ROI Model Assumptions
Fully Loaded Annual Cost of Test Engineer	\$90,000
Percentage of Total Bugs that are Protocol Bugs	30%
Mean Time to Repair a Bug in the Requirement/Architecture/Design Phase of the Development lifecycle	1.2 Hours ⁵
Total Bugs in Software Development Lifecycle for a Release	5000

Table 3
Key Assumptions for the ROI Model

Using these assumptions, the number of protocol software bugs detected and fixed in each stage of the development lifecycle is calculated. NSP calculated this model through multiplying the percentages in Table 2 by 30% (the percentage of total bugs that we assume to be protocol bugs).

⁵ This assumption of 1.2 hours to fix a bug in the first stage phase of the development lifecycle was obtained from the NIST report on *The Economic Impacts of Inadequate Infrastructure for Software Testing*.

The Mu-4000 is very useful throughout the integration and system test portion of the software development lifecycle (SDLC). During the SDLC, the Mu-4000 integrated analysis documentation and vulnerability replay capabilities expedite the repair of most protocol bugs.

Table 4 summarizes the results of these calculations and applies both third-party Mu code coverage metrics and first-hand SDLC knowledge from NSP Partners principals. These calculations find that only 2% of the protocol bugs remain undetected (1% undetected from the Beta Phase and 1% undetected after general availability).

Development Stage	Protocol Bug Distribution without Mu-4000 Testing	Protocol Bug Distribution after Mu-4000 testing
Requirements Gathering and Analysis / Architecture Design	4.5%	4.5%
Coding / Unit Test	6%	6%
Integration and System Test	12%	17.5%
Beta Test	4.5%	1%
General Availability	3%	1%

Table 4
Distribution of Protocol Bug Detection in Each Phase of the Development Lifecycle

Using the results in Table 4 and the assumptions in Table 3, the total cost of bug fixing in each stage of the release is calculated for two cases: 1) a standard test and integration stage where protocol robustness and vulnerability testing are not implemented, and 2) a test and integration stage in which the Mu-4000 is being used to do protocol robustness and vulnerability testing. These results are summarized in Table 5.

Development Stage	Total Bug Fixing Cost without Mu-4000 Testing	Total Bug Fixing Cost with the Mu-4000 testing
Requirements Gathering and Analysis / Architecture Design	\$38,942	\$38,942
Coding / Unit Test	\$259,615	\$259,615
Integration and System Test	\$1,038,462	\$1,067,668
Beta Test	\$584,135	\$447,837
General Availability	\$778,846	\$623,077
Total	\$2,700,000	\$2,437,139

Table 5
Total Bug Fixing Cost in each Stage of the Development Lifecycle with and without the Mu-4000

Using the Mu-4000 vs. not using a Mu-4000 provides a significant cost savings of \$262,861 because it is less expensive to find and fix bugs as early as possible in the development process. Besides building a higher-quality service or product, this translates into the cost of a Mu-4000 appliance being repaid in only one software release cycle. Strong ROI is achieved quickly.

Cost Benefits of Early Vulnerability Detection for Service Providers

Many service providers run network hardware and software through a rigorous test and certification process prior to deployment in their production network. The cost to service providers of finding and fixing product weaknesses including bugs and robustness deficiencies in this test and certification phase is many-times less expensive than the cost of finding and fixing bugs after products are deployed in the production network. Using models parallel to the preceding vendor-specific section and some similar basic assumptions, a calculation is made of the distribution of protocol bugs in each phase of the software development process. These results are presented in Table 6.

In this example, the service provider uses the Mu-4000 to find product vulnerabilities in the Beta test phase of the project. Based upon first-hand Mu customer metrics, NSP Partner SDLC experience and third-party Mu code coverage analysis, we estimate less than 1% of the protocol bugs are not detected by the Mu-4000 based service provider testing during the Beta phase. We also assume that the average time for a service provider test engineer to find bugs, interact with the vendor, and verify fixes is eight hours.

Development Stage	Protocol Bug Distribution without Service Provider Mu-4000 Testing	Protocol Bug Distribution after Service Provider Mu-4000 testing
Requirements Gathering and Analysis / Architecture Design	4.5%	4.5%
Coding / Unit Test	6%	6%
Integration and System Test	12%	12%
Beta Test	4.5%	6.5%
General Availability	3%	1%

Table 6

Protocol Bug Distribution over the Release Cycle showing Service Providers using the Mu-4000 in Test and Certification vs. those not using the Mu-4000

The calculations show that, on average, service providers save nearly \$100,000 (e.g. \$97,356) in each release cycle due to early bug detection, thus, paying back the majority of a service provider's Mu-4000 cost in only one-product deployment. The details of these results are summarized in Table 7.

Development Stage	Total Service Provider Bug Detection and Remediation Cost without Mu-4000 Testing	Total Service Provider Bug Detection and Remediation Cost with Mu-4000 Testing
Requirements Gathering and Analysis / Architecture Design	N/A	N/A
Coding / Unit Test	N/A	N/A
Integration and System Test	N/A	N/A
Beta Test	\$259,615	\$266,106
General Availability	\$519,231	\$415,385
Total	\$778,846	\$681,490

Table 7

Service Provider Bug Detection and Remediation Costs in the Beta Test and Certification Phase vs. Detection of Bugs in the Production Network

Case Studies: Real-World Numbers and Mu-4000 Use Cases

This section of the paper presents case studies of four Mu-4000 analyzer appliance customers. In these case studies NSP details why and how customers use their Mu-4000s and discuss both the ROI and TCO benefits of doing protocol robustness and vulnerability analysis. The proactive use of the [Mu-4000 analyzer appliance](#) increases financial benefits underlying your unique ROI analysis and optimizes your Total Cost of Ownership.

- Network outages in service provider, critical infrastructure, and enterprise networks result in high costs: The Mu-4000 improves service availability through robustness analysis of network elements.
- Finding and fixing bugs as early as possible in both Enterprise and product vendor development lifecycles is significantly less expensive than in a production network.
- The Mu-4000 helps both service providers and network equipment manufacturers find robustness weaknesses, vulnerabilities and response time problems before products and services are deployed in production.

A Tier One Service Provider

A major cable triple-play multi-service operator actively uses the Mu-4000 to improve security testing of any network equipment – and after only a year has achieved many business benefits. Before purchasing a number of Mu-4000 appliances, this operator employed three staff security experts who spent between 20–40% of their time on security testing. These are expensive resources that are not only difficult to initially hire but also replicate those learned skill sets throughout an organization to perform security analysis.

After purchasing its first Mu-4000, the Cable Service Provider began leveraging existing test engineers to spend essentially 100% of their time testing with the Mu-4000. Because of Mu's shareable templates, automation and ability to capture and leverage organization and product-specific staff expertise, the cable provider ultimately needs fewer staff that come up to speed more quickly. Staff leverage and distributed expertise delivers immediate ROI savings over having to hire several additional test engineers. With the Mu-4000's integrated automation and regression analysis, staff time is spent interpreting results, working with the vendors, and defining new test requirements. The Mu-4000 performs the "heavy lifting" of actually running the tests and gathering detailed reporting data. More importantly, the Cable Service Provider estimates that they are now achieving ten times greater test coverage compared to the coverage it was getting using the three expensive security experts.



The security experts at this operator previously used their expert knowledge, homegrown scripts, and other open source tools to test for security weaknesses. Since they did not have an automated Mu-4000 appliance, the problems they found were relatively obvious and most subtle security flaws went undetected. After using the Mu-4000 to perform protocol mutation testing the Cable Service Provider 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. Locating, diagnosing and remediating these problems with existing manual testing framework employed by the security experts would have been nearly impossible.

Also, in the past, a specialized security group did all security testing. However, the regular product certification testing organization did not have a sufficient number of security-testing experts and therefore did not test for security. Without the Mu-4000 it would have been impossible to add security metrics to this organization. By handing off testing using a second Mu-4000 system and another junior engineer, the senior security experts have been redeployed to security architecture, assessment, design, and planning for new revenue-generating services.

This is another way the Mu-4000 provides the operator with a better use of their expertise and keeps them happier in their jobs improving chances of retaining these resources. Also, the security group now defines testing criteria and disseminates sharable testing templates to the other organizations to ensure a common set of operationally relevant comparable testing criteria. The Cable operator is now also using the Mu-4000 for new product evaluation. By finding vulnerabilities as early as possible in the product evaluation cycle it saves time and money in service deployment (as opposed to finding problems late in the cycle or in production).

Another Tier One Service Provider

This service provider provides fixed and mobile voice, data, video, and Internet services to millions of residential and business customers. It has a large security team and does rigorous testing of products in its labs. Before purchasing the Mu-4000 it had multiple challenges including:

- An inability to assess and quantify the effects of protocol fuzzing on the product under test
- An inability to test how effective firewalls, IDPs, and other signature-based security enforcement devices block published or known vulnerabilities
- Labor-intensive and time-consuming security testing outpacing staff on hand and planned budget staff expenditures

After evaluating multiple security test vendors, the service provider selected Mu Dynamics because of its unparalleled capability for comprehensive protocol negative testing using its protocol mutation engine, the ability to test using published vulnerabilities, its automation capabilities, ease of use, and comprehensive remediation reporting.

The service provider currently uses several Mu-4000 systems in disparate locations for:

- **Product Selection:** Evaluating products from multiple vendors before and after purchase for deployment in the network based on protocol robustness.
- **Development Testing:** Determine vulnerabilities and risks associated with new applications and network service configurations, and using reports and tools to remediate problems.
- **Improving Vendors' Product Quality:** Work with vendors to fix protocol vulnerabilities and make their products — and as a result, their own service offerings — more robust.
- **Product Deployment:** Ensure that products and software releases deployed in the production network are robust to protocol vulnerabilities.



For this service provider, the Mu-4000 provides a framework for automated negative testing, greatly increasing the efficiency and scope of their protocol testing. The results include proven operational improvements of their business including higher levels of service availability and a more efficient and comprehensive test and certification process.

SonicWALL

SonicWALL, a leading secure infrastructure company who uses Mu-4000's Published Vulnerability Analysis (PVA) subscription service to improve their product's IDP signature capabilities to better root out network-borne vulnerabilities.

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. Problems in production networks also results in negative press coverage and a degraded reputation among customers, both of which can devastate business.

Before deploying the Mu-4000, SonicWALL used brute-force manpower, homegrown 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 nearly 60% PVA test coverage. 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 detailed remediation tools that streamline the interaction between QA and Engineering, SonicWALL finds it much easier for developers to reproduce and fix problems. This allows developers to fix problems in hours instead of days (or weeks for some problems). 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 PVA score.

The Mu-4000 is also being used for competitive analysis. By applying the appliance to analyze competing products in its test lab, SonicWALL gains important competitive intelligence information that allows account managers and sales engineers to undermine the competition and close competitive information in deals more quickly. Account managers and sales engineers are currently working on a \$500K deal where competitive information derived from the Mu-4000 is being used to help close the sale.

SonicWALL knows IP-borne threats have 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.

An Application Security Vendor

This Fortune *100 Fastest-Growing Company* developer sells software and network appliances that help enterprises improve application security, optimization, and availability. Rather than the expense of building these capabilities internally, many firms such as this developer are purchasing quickly deployed analyzer appliances. The Mu-4000 is also used as part of the vendor's SQA test process. The key benefit of buy vs. build is also manifest in quicker time to market with capabilities that ultimately deliver higher quality products. The engineering team's use of the analyzer throughout the software development lifecycle includes protocol robustness testing to identify and repair bugs before software is released. Many product developers are calculating that the cost of purchasing and deploying a Mu-4000 analyzer is far lower than internally developing similar tools/framework on their own. The added benefit of leveraging Mu's award-winning and service-provider proven expertise in testing standardized communications and software systems.

Analyzing even standards-based software is important because:

- Protocol bugs in production networks result in customer product quality concerns and negative press coverage which often has serious financial consequences
- The cost of finding and fixing bugs in a production network is one to several orders of magnitude higher than fixing bugs in QA (or earlier):
 - Systems engineers must get involved and work the problem
 - Customer support must reproduce bugs
 - Sustaining engineering must reproduce and fix bugs

The vendor's key reasons for using the Mu-4000 are:

- To improve the quality of SQA testing and improve customer satisfaction
- The protocol mutation capabilities are excellent, dynamic and offer superior code coverage
- Sophisticated monitoring and reporting allows engineers and managers to identify and track problems
- Linux executables and PCAP files help developers reproduce and fix bugs quickly

Before deploying the Mu-4000, the vendor performed manual protocol testing using scripts and open source code. With this approach it could find and fix only the most obvious problems. The Mu-4000, however, allows the vendor to achieve significantly higher code coverage, finding subtle corner cases and find hidden boundary conditions, and reach previously unknown corner cases. Serious bugs causing system crashes have been identified and fixed before releasing the product resulting in higher customer quality and lower support costs with far fewer field fire drills.

Conclusion

IP networks are increasingly critical components of every business, network service and even the nation's infrastructure. Business and consumer voice, video, cellular, and Internet services are all carried over increasingly standards-based IP. Service providers, Cable Operators and their diverse IP-enabled product suppliers are all part of the same ecosystem that stresses product quality and, maximum uptime to avoid revenue losses or from customer churn. Additionally, many service providers conduct their businesses every day using IP products containing standards-based and open source components. Even SCADA-based and other industrial networks controlling the electric power grid and MMS, ModBus or DNP systems networks controlling critical chemical, materials, oil, gas and manufacturing processes (respectively) use IP networking technology.

Ensuring the quality, safety and robustness of these product's underlying protocol implementations against vulnerabilities is essential to business security and stability. For this reason, more and more leading service operators are working with their product vendors to carry out protocol robustness testing on any network to ensure that their products and services can withstand malicious attacks as well as innocent user errors.

In summary, the Mu-4000 analyzer appliance offers automated security analysis and testing through an integrated approach to protocol robustness testing, monitoring, and reporting of protocol bugs and vulnerabilities. The Mu-4000 produces a quickly achieved ROI and lower product deployment cost of ownership by significantly reducing costs throughout the product lifecycle and allowing organizations to methodically find and fix bugs early in the process before damages are done. Service providers, product vendors, critical infrastructure operators as well as enterprises depend on the Mu Dynamics solution to maximize application availability, reduce service disruptions, and minimize business risk exposures.

About Mu Dynamics

Mu Dynamics is a technology innovator that has created a new class of security analysis system. The company's mission is to widely deploy security analysis and reduce product and application vulnerabilities. The security analysis process and the Mu-4000 analyzer platform provide a rigorous and streamlined methodology for verifying and improving the service availability and security readiness of any IP-based product or application.

Mu Dynamics enables enterprises and service providers to evaluate new products and software updates for known and previously undetected security vulnerabilities. In so doing, the company:

- Introduces security readiness as a metric for end-users' product purchase and deployment decisions;
- Allows development teams to efficiently identify security flaws in their products before release;
- Significantly decreases the number of security events in production networks through a proactive methodology that detects security flaws before systems and applications are deployed.

Mu Dynamics was founded in 2005 by experts in intrusion detection and prevention, ethical hacking and network management. The company is headquartered in Sunnyvale, California, and is backed by preeminent venture capital firms, including Accel Partners, Benchmark Capital and DAG Ventures.

About Network Strategy Partners, LLC (NSP)

Management Consultants to the networking industry – helps service providers, enterprises, and equipment vendors around the globe make strategic decisions, mitigate risk and affect change through custom consulting engagements. NSP's consulting includes business case and ROI analysis, go-to-market strategies, development of new service offers, pricing and bundling as well as infrastructure consulting. NSP's consultants are respected thought-leaders in the networking industry and influence its direction through confidential engagements for industry leaders and through public appearances, whitepapers, and trade magazine articles. Contact NSP at www.nspllc.com.

