

MARKET OVERVIEW/KEY CHALLENGES

The security and service availability test equipment market has a broad range of addressable markets. Critical assets of businesses are now accessible through an IP network. A wide range of enterprise, government, proprietary and service provider networks are becoming more open. The different kinds of devices and systems on a network are increasing resulting in another level of complexity. Network availability is critical to all business operations and downtime causes loss of profitability, negative publicity, etc. As a result, robust networks are not an option but a necessity and security analyzers provide a methodical process for ensuring that networks are robust, secure and available. To initiate Frost & Sullivan's market coverage of this six-part emerging multi-billion dollar market, we will start with the Security Products segment. Additional segment discussion is noted in chart I.I and will occur in future reports.

Firewall Test Equipment

These products test, measure, analyze or monitor firewall or other defense-in-depth security systems on a single platform. A firewall is a system or group of systems that enforces an access control policy between networks.

VPN Test Equipment

This kind of equipment tests and documents weakness or robustness issues in both Internet protocol security virtual private networks (e.g., IPsec and secure sockets layer (SSL) virtual private network VPN). A VPN is a virtual private communication network comprised of cryptographically protected tunnels through a shared or public network platform such as the Internet.

Intrusion Detection and Prevention Test Equipment

These devices gather and analyze information from various areas within a computer or a network, by using intelligent detection methods to identify possible security breaches.

By testing a network security infrastructure with actual published vulnerability attacks, including deep-packet inspection products,

Chart I.I. FROST & SULLIVAN'S COVERAGE OF THE NEW SIX-PART MULTI-BILLION DOLLAR SECURITY ANALYZER MARKETSPACE INCLUDES:

1. **Security Products**
 - a. Firewalls
 - b. Virtual Private Networks (VPN)
 - c. Intrusion Detection and Prevention
2. **VoIP Products**
 - a. IP PBXs
 - b. Session Border Controllers (SBC)
 - c. IMS products
3. **Networking Products**
 - a. Switches, Routers, Hubs
 - b. Network Access Control
 - c. Storage
 - d. Mobile Wireless and WiMAX
4. **Critical Infrastructure**
 - a. SCADA-based network products (e.g., programmable logic controllers)
 - b. MESH devices
5. **Service Providers**
 - a. Product comparison
 - b. Feature certification
 - c. Bug patch verification
6. **Enterprises**
 - a. Product comparison
 - b. Feature certification
 - c. Bug patch verification

IDS/IPS devices, next-generation firewalls, IPsec VPN concentrators, and SSL accelerators, it is possible to benchmark and verify vendor claims of capacity and performance. With the right test, measurement and analysis procedures, both service provider end users and network product developers save time, allocate resources wisely, and receive assurance in a challenging computing environment.

Over the last 12 months, there has been a massive increase in service provider, cable operator, critical infrastructure enterprises and product developer security awareness and related technological changes. Accordingly, in the security test and measurement market, a new generation of platform vendors like Mu Dynamics have added new features to their devices during 2006. The main technological trends vendors faced since 2005 include:

- Zero-day and Published Vulnerability exploit testing
- Repeatable use of existing test and analysis scripts
- Easy-to-use, graphical interface security test and measurement equipment

Zero-Day and Published Vulnerability Exploit Testing

Zero-day exploit testing is a form of analysis that tests for and ideally identifies security vulnerability before hackers discover it.

Published Vulnerability testing during initial product purchase, upgrade or patch deployment studies the effectiveness of the customer's network infrastructure security enforcement devices (e.g., Firewalls and multi-layer security systems, any deep-inspection devices, or Intrusion Prevention Systems, any of which may be signature-based) for the ability to block packets associated with known attacks.

Ordinarily, after someone detects that a software or hardware program containing a potential exposure to exploitation by a hacker, that person or company notifies the vendor so that responsible vulnerability remediation occurs to repair the exposure or defend against its exploitation. Once customers inform their vendors of such flaws, the vendors have a chance to patch the flaw prior to exploit by hackers. The vulnerability's life cycle is ended before it has a chance to do any damage.

Repeatable use of existing test and analysis scripts

There are thousands of scripts and tools (internally developed, free, open source or commercial) in which a customer might have an investment in using, and these tools are great except they are very labor-intensive to use. With External Analysis capabilities, users continue to leverage the investment (in dollars and time spent) by bringing significant automation infrastructure to bear to improve the usability of the tools.

External analysis vastly improves the productivity of IT or lab staff. The Security test and measurement tool drives the external attack tool to facilitate fault isolation. At the same time, the security test and measurement system monitors the Target to determine if a fault has occurred.

Easy-to-Use, Graphically-based Security Test Equipment

End users, such as enterprises and service providers, have shown frustration over the growing complexities in network security solutions and security test devices. Hence, network security companies and test equipment vendors are moving toward easy-to-use tools and solutions.

AWARD CATEGORIES & RELEVANCE

The security test, measurement and analysis equipment market is highly competitive. Frost & Sullivan believes this market will witness high growth during the next ten years from 2006 to 2016. In order to become and remain a market leader across all the segments of such a hazy market scene, test vendors need to have expertise, adopt innovative strategies, and be able to provide effective and leveraged test tools. It is important to launch such products in a timely manner to meet market needs and understand end-user and product developer priorities and requirements. In order to provide complete solutions in the security test equipment market, it is important to offer products that satisfy the needs in the three initial security product segments:

- Firewall test equipment market
- VPN test equipment market
- Intrusion detection and prevention test equipment market

Frost & Sullivan has identified the company offering the most extensive overall product coverage in the security test, measurement and analysis equipment market. Such company sets the standard for other market participants.

2007 GLOBAL SECURITY TEST PRODUCT OF THE YEAR AWARD

Award Description

The Frost & Sullivan Award for Product of the Year is presented each year to the company demonstrating excellence in new products and technologies within their industry. The recipient company has demonstrated innovation by launching a broad line of emerging products and technologies with wide-ranging acceptance from both end users and product developers.

Research Methodology

To choose a recipient of this Award, the analyst team tracks all new product launches, R&D spending, products in development, and new product features and modifications. This is accomplished through interviews with all the market participants, and extensive secondary and technology research. All new products launched and new products in development in each company are compared and evaluated based on the degree of innovation and customer satisfaction. Companies are then ranked by number of new product launches and new products in development.

Measurement Criteria

In addition to the methodology described above, there are specific criteria used to determine final competitor rankings in this industry. The recipient of this Award has excelled based on one or more of the following criteria:

- Significance of new product(s) in their industry
- Competitive advantage of new product(s) in their industry
- Product innovation in terms of unique or revolutionary technology
- Product acceptance in the marketplace
- New product value-added services provided to customers
- Number of competitors with similar product(s)

2007 GLOBAL SECURITY TEST PRODUCT OF THE YEAR AWARD RECIPIENT: MU DYNAMICS

The 2007 Frost & Sullivan Award for Product of the Year in the security test and measurement industry is conferred to Mu Dynamics, Inc. for its product, the Mu-4000 platform. Mu Dynamics created a new concept in security test and analysis devices; the company is shipping the industry's first security analyzer, the Mu-4000. The Mu-4000 scientifically probes products for both known and unknown vulnerabilities. Mu Dynamics' unique methodology, including the patented Protocol Spidering™ technology and the embedded mutate-monitor-manage process, clearly identifies security, robustness and resiliency issues to address, and applies metrics to any IP-based product or service offering.

The Mu-4000 Analyzer

Mu Dynamics' analyzer system satisfies a critical void in the market today. This is one of the first products to probe effectively for exploitable faults, robustness problems or survivability issues caused by improperly layered protocols, existing published vulnerabilities and many other network interdependencies.

The Mu-4000 demonstrates that network security is a process and far beyond products; the new Mu Dynamics analyzer brings the concept of process for every IP-connected software or hardware product. At present, there are too many product attacks for service providers, critical infrastructure operators, and their respective product developers to simply deploy point security solutions. Evidence of this disturbing trend is the escalating multi-billion dollars of capital and time spent deploying security products with an equally skyrocketing growth of vulnerabilities affecting network downtime and associated data theft. Varying product protocol specifications, unique configurations, and inadequate knowledge of triple play or other complex products requires a more sophisticated and automated approach to security and service availability testing. Mu Dynamics' analyzer system not only meets this requirement but also will ultimately help end users and their product developers reduce the number of network-borne vulnerabilities.

The Mu-4000 analyzer is the first security analysis platform to utilize a systematic and repeatable process to identify unknown and known security vulnerabilities in any IP-based system, application or network device without requiring access to any source code.

- The Mu-4000 platform offers a repeatable and complete Security Analysis process: mutate, monitor, and manage.
- Mu-4000 offers a portable and easy to deploy test harness via an extensible platform that enables organizations to add their own suites of external attack vectors.
- Mu Dynamics' system is a self-contained, rack-mountable (2U) appliance that includes four Gigabit Ethernet and two serial ports for interfacing to the targets being analyzed, two power relay plugs for off/on recycling of systems that may lock up during a failure, and both Ethernet and serial management console ports.

Mu-4000, a Unique and Comprehensive Device

The Mu-4000 platform is unique with its ability to support over 50 protocol families, more than 600 published vulnerabilities for the last three years and a wide range of customer-owned test scripts or other external attack vectors. All three of these testing and measurement applications share a common platform or test harness that delivers packet captures, reports, monitors, enables regression testing, and even delivers a software executable application containing faults discovered during any security analysis.

The Mu-4000's approach is much more methodical, repeatable and complete than a hacker. It employs a methodology called Protocol Spidering™, which is an automated means to assess complex, highly interconnected code for security vulnerabilities. Mutations are created using an object-oriented methodology that mirrors the structure of the protocols themselves, including all the interdependent protocols related to a given protocol. The experience of previous hacker attacks is applied methodically to new protocols, for which attacks can be developed rapidly, which allows those protocols and services to gain valuable scrutiny before they are deployed. The result of using security analyzers raises the bar on hackers in terms of the cost of finding new vulnerabilities. In doing so, the Mu-4000 proactively reduces protocol vulnerabilities, and thus greatly improves product and service security, reliability and robustness.

The Perfect Process to Test a Security Exposure

Mu Dynamics uses the attack surface framework originated by Microsoft and Carnegie Mellon University to create the three applications and underlying Mu-4000 analyzer platform functionality. The attack surface approach methodically defines the level of attack or security exposure of IP-based products. By definition, there are three ways to reduce the attack surface:

- Reduce or eliminate targets, enablers, channels, protocols and rights — the traditional security principle of permitting only what is required.
- Restrict the types or instances of attacks — the principle of using firewalls and layered defenses and access rights to limit access.
- Eliminate or reduce the types or instances of vulnerabilities.
- Conduct a systematic security analysis of products. The Mu-4000 enables customers to minimize security risks by systematically reducing the total attack surface of their network products, and it does so by eliminating or reducing the types or instances of vulnerabilities.

New features already available within the Mu-4000 include additional testing protocols and the ability to analyze products using multiple authentication or transport methods, including IPv4 and IPv6. IPv6 is especially noteworthy since it is native to Microsoft's Vista operating system and the transport of choice for many critical infrastructure and government end users. As companies deploy IPv6 they will face greater security risks from a mix of IPv4 and IPv6-based products in their networks. Mu Dynamics' approach dynamically supports all 3 applications (protocol mutations, published vulnerabilities or external analysis scripts) over IPv6 providing complete security analysis, test and measurement for isolating areas of product weakness.

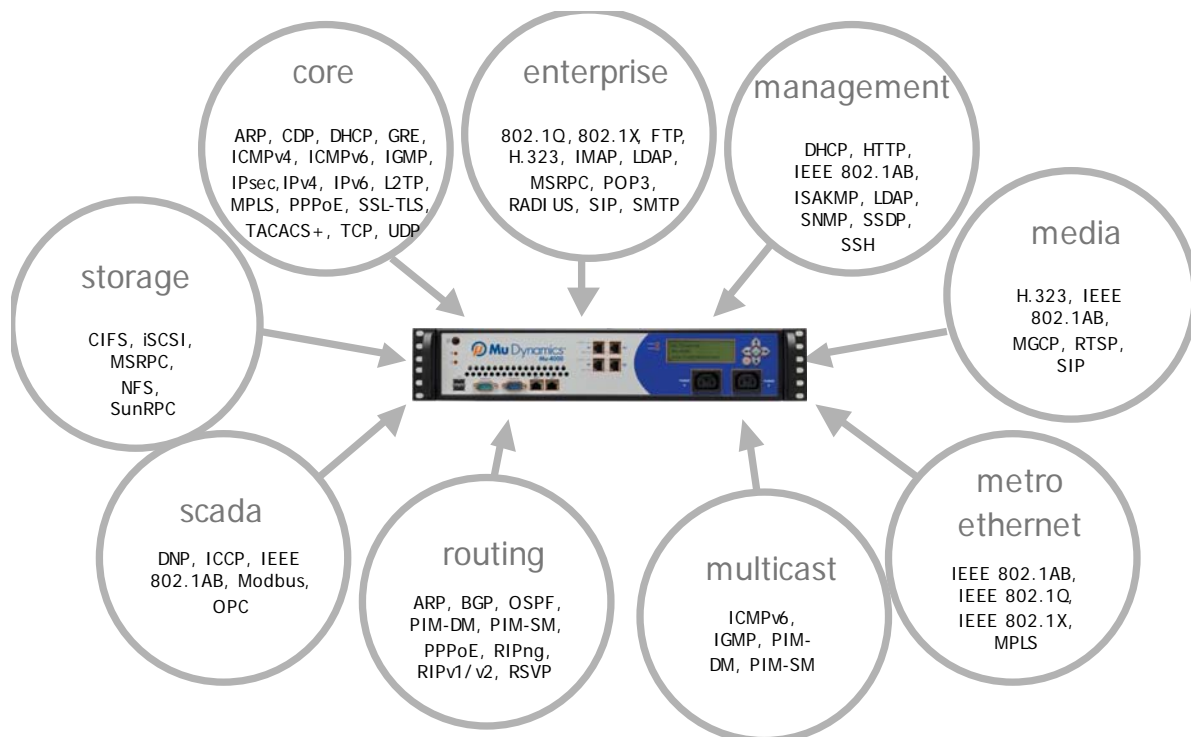


Chart 1.2 shows Mu-4000's protocol coverage in the security test equipment market in the world in 2007.

Vulnerability Test and Documentation for Remediation, Mu-4000's Strengths

Mu Dynamics' Mu-4000 analyzer is a test production lab appliance that launches tens of millions of attacks on any IP-based network product or service prior to deployment, upgrade, patch or other configuration modification. The idea behind Mu Dynamics' approach is to adopt ethical hacking techniques to proactively identify zero-day exploits, thereby minimizing damage to networks.

The Security Analyzer essentially offers its users a vulnerability torture chamber platform, or as some have said, a “tiger team in a box,” that attacks network products using millions of carefully constructed attack vectors that are purpose-built to uncover implementation flaws in the code that implements a given protocol. When there is a failure, the Mu-4000 documents and stores all the information needed to secure the network from that malfunction today and in the future for one-touch repeat (regression) testing or analysis.

Mu-4000, the Right Tool for Many Different End Users

Dozens of Mu-4000 analyzers are already installed in three related yet distinct customer segments. The first includes critical infrastructure and end-user organizations utilizing networking products, such as government agencies, larger enterprises, and service providers that want to assess the comparative security readiness of new solutions or new product releases prior to deployment, upgrade, configuration change or patch incorporation.

The second segment represents networking systems and software vendors who need to metrically evaluate security during product update and development cycles, particularly in the quality assurance testing phase. Many of the end-users in the first category are now asking their product vendors to validate security, robustness or resiliency claims to avoid costly network downtime or customer loss. Some of the users in this segment are requiring their supply chain to adopt the Mu-4000 to prove that the devices meet the requirements for security and service availability.

The third segment consists of independent labs and certification agencies that evaluate networking products, creating a benchmark standard among competitive offerings.

Service providers, critical infrastructure and Government agencies depend on the Mu-4000 to enhance their network uptime or revenue-bearing network services by reducing system downtime that often results in the loss of either existing customers or confidential information, which proves to be very expensive. Mu Dynamics helps end users baseline their wide-ranging products' security and robustness during initial purchase or upgrade to help ensure maximum uptime. To complement existing security personnel, Mu Dynamics automates existing analysis tools and testing processes and boosts staff effectiveness, productivity, and knowledge base. This approach also maximizes network services against disruption or malicious activities. The Mu-4000 is useful during the build out of any triple play or multi-function service offering, security product installation, and mission-critical system ranging from components of manufacturing processes to secure military transport facilities.

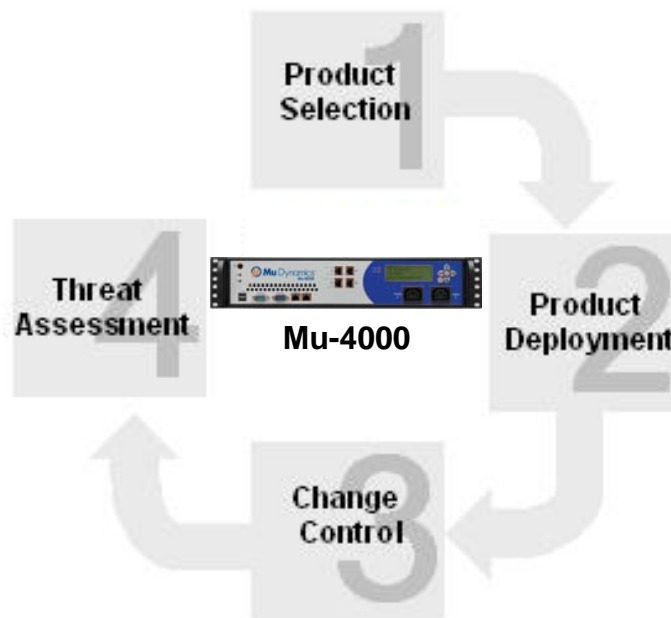


Chart I.3 shows the end-user perspective of the lifecycle of a security analyzer in the security test, analysis and measurement equipment market in the world in 2007.

Product developers including a diverse set of network software and equipment manufacturers use the Mu-4000 platform to ensure their products vulnerable to fewer 0-day and published vulnerability defects that would cause their end user customers to suffer negative public consequences, decline in revenue or customer turnover. The increasing complexities of triple play service deployments, security product rollouts or 3G/wireless services can quickly outpace existing resources' ability to isolate the attack surface of any product deployed within the entire network. Product development QA teams use the Mu-4000 to extend their ability and test coverage expertise for increasingly complex products with the goal of maximizing critical infrastructure or service providers' customer retention. Prior to the introduction of the Mu-4000, there was no automated testing system available to baseline a process for establishing security readiness or robustness.

Mu-4000, a Technological Update in the Security and Service Availability Test Equipment Market

With the Mu-4000, Mu Dynamics is establishing a leadership position in the emerging security test equipment market. Since March 2006, Mu Dynamics has gained dozens of customers ranging from AT&T, Sprint, Motorola, Juniper, Network Appliance, Siemens, ABB Group, US Government agencies, Decru, Veraz, and other industry leaders in the core, enterprise, management, media, metro Ethernet, multicast, routing, SCADA and storage markets. Mu Dynamics will continue to build out its application suite for detailing product resiliency, reliability and survivability using a common test harness and underlying suite of platform applications during the next twelve months.

About Best Practices

Frost & Sullivan Best Practices Awards recognize companies in a variety of regional and global markets for demonstrating outstanding achievement and superior performance in areas such as leadership, technological innovation, customer service, and strategic product development. Industry analysts compare market participants and measure performance through in-depth interviews, analysis, and extensive secondary research in order to identify best practices in the industry.

About Frost & Sullivan

Frost & Sullivan, a global growth consulting company, has been partnering with clients to support the development of innovative strategies for more than 40 years. The company's industry expertise integrates growth consulting, growth partnership services, and corporate management training to identify and develop opportunities. Frost & Sullivan serves an extensive clientele that includes Global 1000 companies, emerging companies, and the investment community by providing comprehensive industry coverage that reflects a unique global perspective and combines ongoing analysis of markets, technologies, econometrics, and demographics. For more information, visit www.frost.com.

Mu-4000; a Complete Success in the Security Test Equipment Market

In conclusion, Mu Dynamics is adopting a unique and repeatable approach to security analysis, by using techniques similar to those employed by hackers to eliminate vulnerabilities in network products. The company has in-depth knowledge on attack surface coverage weaknesses, network vulnerabilities and strives to meet its customers' wide-ranging requirements in every aspect and in the different segments of the security test and measurement equipment market including the initial part of Frost & Sullivan's product area coverage:

- Firewall test equipment market
- VPN test equipment market
- Instruction detection and prevention test equipment market

With the Mu-4000 analyzer, Mu Dynamics is being explicitly appreciated by end users in the market for its expertise, and exhibits a great degree of adaptability, in sync with market dynamics, customizing its solutions to clients' requirements. In recognition of the above-mentioned factors, Frost & Sullivan proudly presents the 2007 Product of the Year Award to Mu Dynamics, Inc.