

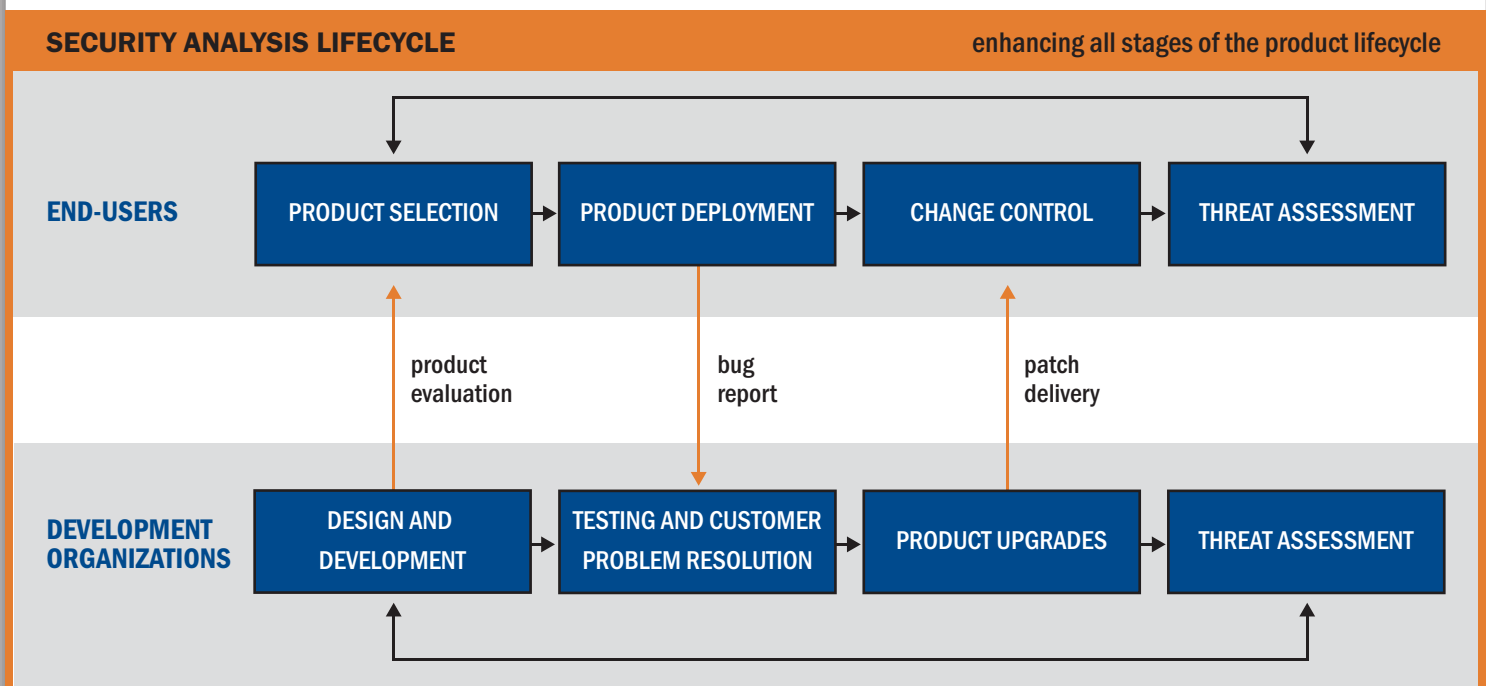
Value Proposition

Mu Security delivers a rigorous and highly customizable security analysis solution to proactively improve the security and robustness of any IP-based hardware or software product throughout its development and/or deployment lifecycles.

End-users have limited visibility into the true security stance of any IP-based product they are purchasing or upgrading. Security analysis provides these end-users with a measurable means to understand a product's security readiness before production deployment, as well as the ability to hold vendors accountable for insecure products.

Development organizations typically lack security expertise and effective security tools in the product development or quality assurance groups. As a result, products are not security-ready before they are released to end-user customers. Security analysis improves the product development process, enabling developers to produce products and applications that are less vulnerable to hacker attempts.

Mu Security's solution addresses inherent weaknesses in the reactive, layered-defense approaches to security, which have not fundamentally improved security in the last two decades. The Mu-4000 Security Analyzer delivers significant productivity gains, cost savings and tangible security improvements to both end-user customers and development organizations.



Security Analysis Lifecycle

Security is a process of continuous improvement, and security analysis provides an underlying context in which security can be measured and therefore managed. The Mu Security methodology is easily embedded within the entire lifecycles of both development organizations and end-users, ensuring that any IP-based system is inoculated against a broad set of published and 0-day vulnerabilities.

END-USERS

- **Product Selection:** Security readiness should be a key metric to support purchase decisions, in addition to functionality and performance.
- **Product Deployment:** When new features and functionality are activated, or changes are introduced into the network architecture, end-users should proactively identify and remove vulnerabilities before deployment.
- **Change Control:** Before a new software release or a bug fix is rolled out, end-users ought to ensure that no published or previously eliminated vulnerabilities are inadvertently reintroduced into a stable environment.
- **Threat Assessment:** Security crisis management and problem reporting to a vendor is streamlined with Mu-4000's ability to automate and "operationalize" the vulnerability remediation process.

DEVELOPMENT ORGANIZATIONS

- **Design and Development:** Developers should repair security flaws as early as possible in the development process, where bug fixing is far less costly than in released code.
- **Testing and Customer Problem Resolution:** Mutations boost the predictive power and regression coverage over existing tests. Information captured by the Mu-4000 brings quick focus to addressing customer-reported problems rather than struggling to reproduce them reliably.
- **Software Upgrades:** Assessment of configuration changes, software updates and patches to ensure that security regressions are not introduced.
- **Threat Assessment:** Verification of correct and effective operation of production network security products for specific configurations.

Products

The Mu-4000 Security Analyzer is a security analysis platform that delivers the industry's first systematic and repeatable process to identify unknown and published vulnerabilities in any IP-based system, application or network device without requiring access to source code.

The Mu-4000 offers the users a complete security analysis process (**mutate, monitor and manage**) that easily integrates with their existing efforts. The Mu-4000 subjects the target under analysis to a virtually unlimited number of attack vectors (the mutations), monitors the target, and captures the results in a database, all while managing the process in a reproducible and actionable manner, including producing output and utilities to speed fault remediation. This lifecycle approach enables the creation of security-enabled processes in all phases of product development as well as deployment.

The Mu-4000's extensible security analysis platform also enables organizations to integrate their own suites of attacks. The Security Analyzer is a self-contained, rack-mountable appliance that is easily configured and managed.

MU-4000 PRODUCT SPECIFICATIONS

PLATFORM FEATURES

Mu-developed Attacks

Generates millions of mutations (attacks) based on Mu Security's deep understanding of security, hacker methodology and secure programming techniques.

External Attacks

Support for customer developed attack scripts to allow continued leverage of their installed base of attack vectors with Mu Security's extensive set of Monitors and Managers.

Published Vulnerability Analysis

Allows customers to test in a timely manner the security readiness of networking software and hardware products against critical vulnerabilities published on the Internet by a wide variety of sources.

MU-4000 SECURITY ANALYZER



External Vulnerability Triggers

The Mu-4000 Security Analyzer can generate an independently executable program for reproducing faults without needing access to a Mu-4000 system.

Monitors

Monitors the target under analysis using a variety of methods including SSH, TELNET, Console, SYSLOG, Custom CLI (including running inside a debugger). Monitors can work with targets with monolithic or process-based architectures.

Managers

Takes action based on information discovered by Monitors to reset the target to a state that allows for root cause discovery and continued testing with no human intervention – these include hardware managers for device restarts and software managers for power-unit-based and process restarts. Also there is an extremely flexible framework for interfacing with external attack generators.

Reporting

An on-board database coupled with sophisticated report generation tools generates reports meeting a wide range of needs. Summary reports for engineering management, detailed reports for security experts and fault reports for developers are generated with ease.

HARDWARE

Chassis

2U, 19" rack-mount 3.5 x 17 x 15 in.
(8.6 x 43 x 38.1 cm.)

Weight

22 lbs. (10 kilograms)

Power

100 – 240V AC, 50/60Hz, 4.5A auto-ranging

Annunciators

LCD panel with selector switch panel

Storage

Dual on-board hard drives and DVD/CD-RW drive

Environmentals

- Operating temp: 32 to 104 °F (0 to 40 °C)
- Storage: -4 to 158 °F (-20 to +70 °C)
- Operating or storage relative humidity: 5 to 95%, non-condensing

Connectors

- 2 Gigabit Ethernet management ports; auto-negotiating, RJ45 connectors
- 2 Serial Console interfaces (RS-232 DB9 connectors)
- 4 Gigabit Ethernet attack ports; auto-negotiating, RJ45 connectors
- 2 power relay connectors on front panel, 2 on rear panel

Agency Approvals

CE Mark, FCC Part 15 Class A

PROTOCOLS

The following is a list of protocols supported. Please check with your Mu Security representative for the latest and complete list of supported protocols:

- ARP (Address Resolution Protocol)
- BGP4 (Border Gateway Protocol version 4)
- CDP (Cisco Discovery Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transport Protocol)
- ICMP (Internet Control Message Protocol)
- IGMP (Internet Group Management Protocol)
- IMAP (Internet Message Access Protocol)
- IPv4 (Internet Protocol version 4)
- IPv6 (Internet Protocol version 6)
- ISAKMP (Internet Security Association and Key Management Protocol)
- LDAP (Lightweight Directory Access Protocol)
- PIM-DM (Protocol Independent Multicast – Dense Mode)
- PIM-SM (Protocol Independent Multicast – Sparse Mode)
- POP3 (Post Office Protocol version 3)
- RADIUS (with Cisco, Juniper and Microsoft Extensions)
- RTSP (Real Time Streaming Protocol)
- SIP (Session Initiation Protocol)
- SMTP (Simple Mail Transfer Protocol)
- SNMP (Simple Network Management Protocol) and SNMP Traps
- SSDP (Simple Service Discovery Protocol)
- SSH (Secure Shell)
- Sun RPC (Remote Procedure Call) and Portmapper
- TCP (Transmission Control Protocol)
- TFTP (Trivial File Transfer Protocol)
- TLSv1 (Transport Layer Security version 1)
- UDP (User Datagram Protocol)

COMPETITIVE MATRIX

Security Analysis Requirements	Mu-4000 Security Analyzer	Protocol Fuzzer	VA Scanner*	Web Application Scanner**	Source Code Analyzer	Penetration Test Tools
Identification of 0-day protocol implementation flaws	●	●	○	○	○	○
Full spectrum of attacks (vendor-generated, customer-generated and published attacks)	●	◐	◐	◐	◐	◐
Active exploitation of published vulnerabilities	◐	○	◐	●	○	●
No source code or binaries required for analysis	●	●	●	●	○	●
Application-layer security analysis	◐	○	◐	●	◐	◐
Fully-automated published and 0-day vulnerability analysis, including expedited remediation and regression processes	●	◐	◐	◐	○	◐
Expedite remediation for 0-day vulnerabilities	●	○	○	○	○	○
Seamless integration with external security and robustness scripts, tools and third-party applications	●	○	○	◐	○	○
Integrated database for automated regression and trending	●	○	◐	◐	◐	○
Streamlined vulnerability information exchange between vendors and end-users	●	◐	◐	◐	○	○

*Patched vulnerabilities only

**Web protocols only

● yes ◐ partial ○ no

NOTE: Patch management product solutions are also used by both product developers and end-users but do not significantly address any of these security analysis characteristics

About Mu Security

Mu Security offers a new class of security analysis system, delivering a rigorous and streamlined methodology for verifying the robustness and security readiness of any IP-based product or application. Founded by pioneers of intrusion detection and prevention technology, Mu Security is backed by preeminent venture capital firms including Accel Partners, Benchmark Capital and DAG Ventures. For more information, visit the company's website at <http://www.musecurity.com>.



web: www.musecurity.com | email: info@musecurity.com
 address: 1153 Bordeaux Drive, Suite 102, Sunnyvale, CA 94089, USA
 phone: (866) 276-4640 or (408) 329-6330 | fax: (408) 329-6317