Cisco Security Monitoring, Analysis, and Response System (MARS) Release 6.0

Cisco Security MARS Overview

Cisco Security MARS is an appliance-based, all-inclusive solution that provides superior insight into and control of your existing security deployment. Part of Cisco's security management suite, Cisco Security MARS empowers your security and network organizations to identify, manage, and counter security threats. It works with your existing network and security investments to identify, isolate, and recommend precise removal of offending elements. Cisco Security MARS also helps maintain internal policy compliance and can be an integral part of your overall regulatory compliance solution.

Security and network administrators face numerous challenges, including:

- Security and network information overload
- Poor attack and fault identification, prioritization, and response
- Increases in attack sophistication, velocity, and remediation costs
- Compliance and audit requirement adherence
- Security staff and budget constraints
- Cisco Security MARS addresses these challenges by:
- Integrating network intelligence to modernize correlation of network anomalies and security events
- Visualizing validated incidents and automating investigation
- Mitigating attacks by taking full advantage of your existing network and security infrastructure
- Monitoring systems, network, and security operations to aid in compliance
- Delivering a scalable appliance that is easy to deploy and use with the lowest total cost of ownership (TCO)

Cisco Security MARS transforms raw network and security data into intelligence that can be used to subvert valid security incidents and maintain compliance. Cisco Security MARS enables operators to centralize, detect, mitigate, and report on priority threats using the network and security devices already deployed in your infrastructure.

The Defense-in-Depth Dilemma

Information security practices have evolved from Internet perimeter protection to an in-depth defense model in which multiple countermeasures are layered throughout the infrastructure to address vulnerabilities and attacks. Layering is necessary because of increased attack frequency, diverse attack sophistication, and the rapid nature of attack velocity.

Network access points and systems are probed thousands of times each day in an attempt to exploit vulnerabilities. Modern blended/hybrid attacks use multiple and deceptive attack methodologies to gain unauthorized system access and control from outside and within

organizations. The proliferation of worms, day-zero attacks, viruses, Trojan horses, spyware, and attack tools challenges even the most fortified infrastructures, resulting in shorter reaction time and costly remediation.

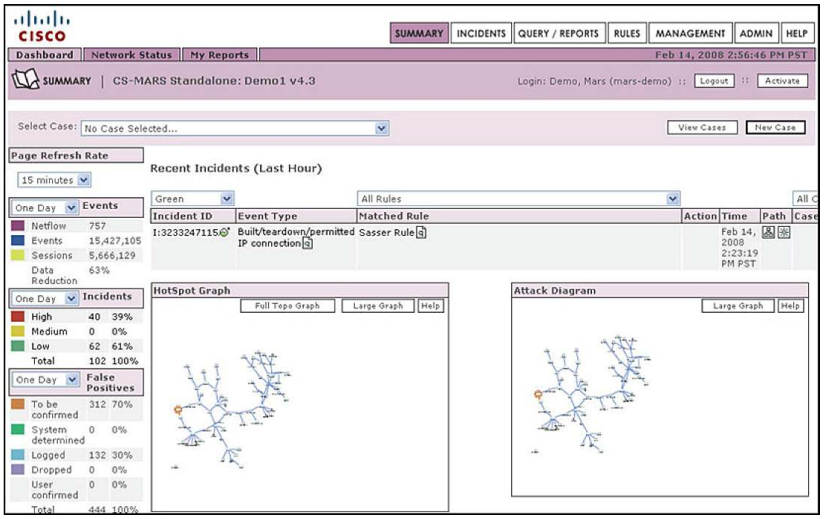
In addition to the number of servers and network devices, each security component offers isolated event log and alert features for anomaly detection, threat reaction, and forensics. Unfortunately, this isolation yields a tremendous amount of noise, alarms, log files, and false positives for operators to discern or effectively utilize. In addition, compliance legislature requires strict data privacy, improved operational security, and documented audit processes.

Advancing Security Information Management and Threat Mitigation

Security information and event management products logically seem to alleviate these problems—helping you measure threats so you can manage them. These products enable operators to centrally aggregate security events and logs, analyze this data through limited correlation and query techniques, and generate alarms and reports about isolated events.

Unfortunately, many first-generation and second-generation security information and event management products do not yield sufficient network intelligence and performance attributes to precisely identify and validate correlated events, specifically determine attack paths, or precisely remove threats. Cisco addresses these security issues and management deficiencies with a family of scalable enterprise threat mitigation appliances. Cisco Security MARS complements your network and security infrastructure investment by delivering a security threat control and containment solution that is easy to deploy, easy to use, and cost-effective. The Cisco Security MARS family of high-performance, scalable threat mitigation appliances fortifies deployed network devices and security countermeasures by combining network intelligence, ContextCorrelation™ features, SureVector™ analysis, and AutoMitigate™ capability, which empower organizations to readily identify, manage, and eliminate network attacks and maintain compliance.
Cisco Security MARS tightly integrates with Cisco's premier security management configuration product, Cisco Security Manager. This integration maps traffic-related syslog messages to the firewall policies defined in Cisco Security Manager that triggered the event. Policy lookup enables rapid, round-trip analysis for troubleshooting firewall-configuration-related network issues and configuration errors.

Figure 1. Shows the MARS Dashboard page with a Summary of Current Security Posture



Features and Benefits

Intelligent Event Aggregation and Performance Processing

Cisco Security MARS obtains network intelligence by understanding the network topology and device configurations and by profiling network traffic. The system's integrated network discovery function builds a topology map containing device configuration and current security policies, which enables Cisco Security MARS to model packet flows through your network. Since Cisco Security MARS does not operate inline and makes minimal use of existing software agents, there is little negative effect on network or system performance.

Cisco Security MARS centrally aggregates logs and events from a wide range of popular network devices (such as routers and switches), security devices and applications (such as firewalls, intrusion detection systems [IDSs], vulnerability scanners, and antivirus applications), hosts (such as Windows, Solaris, and Linux syslogs), applications (such as databases, Web servers, and authentication servers), and network traffic (such as Cisco NetFlow).

Cisco ContextCorrelation

As events and data are received, the information is normalized against the topology, discovered device configurations, and same source and destination applications across Network Address Translation (NAT) boundaries. Corresponding events are grouped into sessions in real time. System- and user-defined correlation rules are then applied to multiple sessions to identify incidents. Cisco Security MARS ships with a full complement of predefined rules, frequently updated by Cisco, which identify a majority of blended attack scenarios, day-zero attacks, and worms. A graphical rule definition framework simplifies the creation of user-defined custom rules for any application. ContextCorrelation significantly reduces raw event data, facilitates response prioritization, and maximizes results from deployed countermeasures.

High-Performance Aggregation and Consolidation

Cisco Security MARS captures millions of raw events, efficiently classifies incidents with superior data reduction, and compresses this information for archival. Managing this high volume of security events requires a secure and stable centralized logging platform. Cisco Security MARS appliances are security-hardened and optimized for receiving extremely high levels of event traffic: more than 15,000 events per second or more than 300,000 Cisco NetFlow events per second. This high-performance correlation is made possible through inline processing logic and the use of embedded high-performance database systems. All database functions and tuning are transparent to the user. Onboard storage and continual compression of historical data archives to network file system NFS, and Secure File Transfer Protocl (sFTP) secondary storage devices make Cisco Security MARS a reliable security log aggregation solution. MARS also supports data and configuration backup and recovery via NFS, and sFTP.

Incident Visualization and Mitigation

Cisco Security MARS helps to accelerate and simplify the process of threat identification, investigation, validation, and mitigation. Security staff are often confronted with escalated events that require time-consuming analysis for resolution and remediation. Cisco Security MARS provides a powerful, interactive security management dashboard. The operator GUI provides a topology map that includes real-time hotspots, incidents, attack paths, and detailed investigation with full incident disclosure, allowing immediate verification of valid threats.

Cisco SureVector analysis processes similar event sessions to determine if threats are valid or have been countered by assessing the entire attack path, down to the endpoint MAC address. This automated process is accomplished by analyzing device logs such as firewalls and intrusion prevention applications, third-party vulnerability assessment data, and Cisco Security MARS endpoint scans to eliminate false positives. Users can quickly fine-tune the system to further reduce false positives.

The goal of any security program is to keep systems online and functioning properly—this is critical for preventing security exposures, containing incidents, and facilitating remediation. With Cisco Security MARS, operators have a rapid means to understand all of the components involved in an attack, down to the offending and compromised system MAC address. Cisco AutoMitigate capabilities identify available “chokepoint” devices along the attack path and automatically provide the appropriate device commands that the user can employ to mitigate the threat. The results can be used to quickly and accurately prevent or contain an attack.

Real-Time Investigation and Compliance Reporting

Cisco Security MARS features an easy-to-use analysis framework that simplifies the conventional security workflow, providing automated case assignment, investigation, escalation, notification, and annotation for daily operations and specialized audits. Cisco Security MARS can graphically replay attacks and retrieve stored event data to analyze previous events. The system fully supports spontaneous queries for real-time and subsequent data-mining efforts.

Cisco Security MARS offers numerous predefined reports to satisfy operational requirements and assist in regulatory compliance efforts, including compliance with the Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes-Oxley, Gramm-Leach Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Federal Information Security Management Act (FISMA) in the United States; the EU’s Revised Basel Capital Framework (Basel II); and others. An intuitive report generator can modify the more than 100 standard reports or generate new reports for an unlimited means to build action and remediation plans, incident and network activity, security posture and audit, as well as departmental reports—in data, trend, and chart formats. The system also provides for batch and e-mail reporting.

Rapid Deployment and Scalable Management

Cisco Security MARS is placed on a network, where it can send and receive syslog messages and Simple Network Management Protocol (SNMP) traps and can establish secure sessions with deployed network and security devices through standard secure or vendor-specific protocols. No additional hardware, operating system patches, licensing, or lengthy professional service engagements are required to install and deploy Cisco Security MARS. Simply configure your log sources to point to Cisco Security MARS and define any network and source through the Web-based GUI. Cisco Security MARS can also forward syslogs to an external syslog server to integrate with existing network infrastructures.

Cisco Security MARS supports the optional Global Controller appliance which centralizes security Local Controller reporting to provide a single view report aggregation of the enterprise Local Controller environment.

Global Controller Capabilities include:

- Aggregation of reports across the Local Controller deployment

- Defining Rules, Reports and User accounts for Local Controllers (Note: Configuration of Local Controller is done “locally” on the individual LC appliance)
- Remote, distributed upgrade of the Local Controllers

Cisco Security MARS Technical Specifications

Release Information

Cisco Security MARS Release 6.0 is targeted for release August 2008 and will support both first-generation and second-generation hardware platforms at this time. The first-generation platform, which was supported under 4.x releases, will require reimaging to the Release 6.0 images. The second-generation platforms may move through a standard upgrade process to upgrade to this new release.

The Cisco Security MARS family offers different performance characteristics and prices to meet a variety of organizational needs and deployment scenarios (Table 1).

Table 1. Cisco Security MARS Technical Specifications

Cisco Part Number (Local Controller Models)	Events/Sec[1]	NetFlows/Sec	Storage	Rack Unit	Power
Cisco Security MARS 25R (CS-MARS-25R-K9)	75	1500	250 GB (non-RAID)	1 RU x 20 in. (D) x 19 in. (W)	350W, 120/240V autoswitch
Cisco Security MARS 25 (CS-MARS-25-K9)	750	15,000	250 GB (non-RAID)	1 RU x 20 in. (D) x 19 in. (W)	350W, 120/240V autoswitch
Cisco Security MARS 55 (CS-MARS-55-K9)	1500	30,000	500 GB RAID 1	1 RU x 25.5 in. (D) x 19 in. (W)	350W, 120/240V autoswitch
Cisco Security MARS 110R (CS-MARS-110R-K9)	4500	75,000	1500 GB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)	2x 750W dual-redundant, 120/240V autoswitch
Cisco Security MARS 110 (CS-MARS-110-K9)	7500	150,000	1500 GB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)	2x 750W dual-redundant, 120/240V autoswitch
Cisco Security MARS 210 (CS-MARS-210-K9)	15,000	300,000	2000 GB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in (H); 19" (W) in.	2x 750W dual-redundant, 120/240V autoswitch

Cisco Part Number (Global Controller Models)	Local Controller Models Supported	Maximum Connections	Storage	Rack Unit	Power
Cisco Security MARS GC2R (CS-MARS-GC2R-K9)	Cisco Security MARS 20R/20/50 and MARS 25R/25/55 only	5	2 TB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)	2x 750W dual-redundant, 120/240V autoswitch
Cisco Security MARS GC2 (CS-MARS-GC2-K9)	All Cisco Security MARS	Not restricted	2 TB RAID 10 hot-swappable	2 RU x 27.75 in. (D); 3.44 in. (H); 19 in. (W)	2x 750W dual-redundant, 120/240V autoswitch

Dynamic Session-Based Correlation

- Network-based anomaly detection, including Cisco NetFlow
- Behavior-based and rules-based event correlation
- Comprehensive built-in and user-defined rules
- Automated NAT normalization

[1] Events per second: maximum events per second with dynamic correlation and all features enabled.

Topology Discovery

- Layer 3 and Layer 2 routers, switches, and firewalls
- Network IDS blades and appliances
- Manual and scheduled discovery
- Secure Shell (SSH) Protocol, SNMP, Telnet, and device-specific communications

Vulnerability Analysis

- Incident-triggered targeted network-based and host-based fingerprinting
- Switch, router, firewall, and NAT configuration analysis
- Automated vulnerability scanner data capture
- Automated and user-tuned false positive analysis

Incident Analysis and Response

- Role-based security event management dashboard
- Session-based event consolidation with full-rule context
- Graphical attack path visualization with detailed investigation
- Attack path device profiles with endpoint MAC identification
- Graphical and detailed sequential attack pattern display
- Incident details, including rules, raw events, common vulnerabilities and exposures (CVEs), and mitigation options
- Immediate incident investigation and false positive determination
- GUI rule definition in support of custom rules and keyword parsing
- Incident escalation with user-based “to-do” work list
- Notification, including e-mail, pager, syslog, and SNMP
- Integration with existing ticketing and workflow system using Extensible Markup Language (XML) event notification

Query and Reporting

- Low-latency, real-time event query
- GUI that supports numerous default queries and customized queries
- More than 150 popular reports, including management, operational, and regulatory
- Intuitive report generation yielding unlimited customized reports
- Data, chart, and trend formats that support HTML and comma-separated value (CSV) export
- Live, batch, template, and e-mail forwarding reporting system
- Easy-to-use query structure built for an effective navigation to the information in a specific incident

Administration

- Web interface (HTTPS); roles-based administration with defined privileges
- Global Controller hierarchical report consolidation for multiple Cisco Security MARS Local Controller appliances
- Automated, verified updates, including device support, new rules, and features
- Continuous compressed raw data and incident archive to offline NFS storage
- Automated system backup and restore using Secure FTP

Device Support

- Network: Cisco IOS® Software, Cisco Catalyst® OS, Cisco NetFlow, and Extreme Extremeware
- Cisco ASA 5580 adaptive security appliances
- Firewall/VPN: Cisco ASA Software; Cisco PIX® 500 Series Security Appliances; Cisco IOS Firewall; Cisco Firewall Services Module (FWSM); Cisco VPN 3000 Series Concentrators; Checkpoint Firewall-1 NG and VPN-1 versions; NetScreen Firewall; and Nokia Firewall
- Intrusion detection: Cisco IPS; Cisco IDS; Cisco IDS Module; Cisco IOS IPS; Enterasys Dragon NIDS; ISS RealSecure Network Sensor; Snort NIDS; McAfee Intrushield NIDS; Juniper IDP; OS; and Symantec ManHunt
- Vulnerability assessment: eEye REM, QualysGuard, and McAfee FoundStone FoundScan
- Wireless controller: Cisco Wireless LAN Controller Module
- Host security: Cisco Security Agent, McAfee Entercept, and ISS RealSecure Host Sensor
- Antivirus: Symantec Antivirus, Cisco Incident Control System (Cisco ICS), Trend Micro Outbreak Prevention Service (OPS), Network Associates VirusScan, and McAfee ePO
- Authentication servers: Cisco Secure Access Control Server (ACS)
- Host log: Windows NT, 2000, and 2003 (agent and agentless); Solaris; and Linux
- Application: Web servers (Internet Information Server, iPlanet, and Apache), Oracle audit logs, NetApp NetCache, and ISS Site Protector
- Universal device support to aggregate and monitor any application syslog
- Support for additional and custom devices using the custom log parser feature

Cisco Security MARS continues to improve device support. For the comprehensive, up-to-date list with supported release information, see http://www.cisco.com/en/US/products/ps6241/products_device_support_tables_list.html.

Additional Hardware Specifications

- Purpose-built 19-in. rack-mountable appliances; UL, VCCI, CE, and FCC part 15 approved
- Security-hardened OS with firewall with restricted services
- Two 10/100/1000-MB Ethernet interfaces
- DVD-ROM drive with recovery media

Ordering Information

To place an order, visit the Cisco Ordering Home Page. Table 2 lists ordering information for Cisco Security MARS.

Table 2. Cisco Security MARS Ordering Information

Part Number	Cisco SMARTnet Service Part Number	Description
CS-MARS-25R-K9	CON-SNT-MARS25R	Cisco Security MARS 25R
CSMARS-25-LIC-K9=	CON-SNT-MARS25U	Cisco Security MARS 25R upgrade license to CS-MARS-25-K9
CS-MARS-25-K9	CON-SNT-MARS25	Cisco Security MARS 25
CS-MARS-55-K9	CON-SNT-MARS55	Cisco Security MARS 55
CS-MARS-110R-K9	CON-SNT-MARS110R	Cisco Security MARS 110R
CSMARS-110-LIC-K9=	CON-SNT-MARS110U	Cisco Security MARS 110R upgrade license to CS-MARS-110-K9
CS-MARS-110-K9	CON-SNT-MARS110	Cisco Security MARS 110
CS-MARS-210-K9	CON-SNT-MARS210	Cisco Security MARS 210
CS-MARS-GC2R-K9	CON-SNT-MARSGC2R	Cisco Security MARS GC2R
CSMARS-GC2-LIC-K9=	CON-SNT-MARSGC2L	Cisco Security MARS GC2R upgrade license to CS-MARS-GC2-K9
CS-MARS-GC2-K9	CON-SNT-MARSGC2	Cisco Security MARS GC2

Cisco Service and Support

Cisco takes a lifecycle approach to services and, with its partners, provides a broad portfolio of security services so enterprises can design, implement, operate, and optimize network platforms that defend critical business processes against attack and disruption, protect privacy, and support policy and regulatory compliance controls.

Cisco services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. Cisco services include:

- The Cisco Security Center provides one-stop shopping for early warning threat intelligence threat and vulnerability analysis, Cisco IPS signatures, and mitigation techniques. Visit and bookmark the Cisco Security Center at http://www.cisco.com/security.
- The Cisco Security Intellishield Alert Manager Service provides a customizable, Web-based threat and vulnerability alert service that allows organizations to easily access timely, accurate, and credible information about potential vulnerabilities in their environment.
- Cisco Security Optimization Service: Increasingly, the network infrastructure is the foundation of the agile and adaptive business. The Cisco Security Optimization Service supports the continuously evolving security system to meet ever-changing security threats through a combination of planning and assessments, design, performance tuning, and ongoing support for system changes. This service helps integrate security into the core network infrastructure.
- Cisco SMARTnet® Service delivers rapid issue resolution by giving businesses direct, anytime access to Cisco engineers; an award-winning online support center; machine-to-machine diagnostics on select devices; and premium advance hardware replacement options.

- The Cisco Security MARS Implementation Service provides expert network analysis, planning, design, and implementation assistance to help organizations deploy an effective in-depth network defense that speeds attack response capabilities and enhances network and security operations monitoring to aid in compliance activities.

For More Information

For more information about Cisco Security MARS Release 6.0, visit http://www.cisco.com/go/mars or contact your account manager or a Cisco Authorized Partner.

For more information about Cisco Security Manager, visit http://www.cisco.com/go/csmanager.

For more information about Cisco Security Services, visit http://www.cisco.com/en/US/products/svcs/ps2961/ps2952/serv_group_home.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-458671-00 03/08

