Cisco Security Monitoring, Analysis, and Response System 4.3.1/5.3.1

The Cisco® Security Monitoring, Analysis, and Response System (Cisco Security MARS) is an appliance-based, all-inclusive solution that provides unmatched insight and control of your existing security deployment. Part of Cisco's security management lifecycle, 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. It 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. This easy-to-use family of threat mitigation appliances 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. This is necessary due to increased attack frequency, diverse attack sophistication, and the rapid nature of attack velocity—all blurring the boundaries between the network and perimeter.

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 smaller reaction time, downtime, and costly remediation.

Beyond 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 yields a tremendous amount of noise, alarms, log files, and false positives for operators to discern or effectively use—assuming the time and resources are available to parse through and understand this information. In addition, compliance legislature requires strict data privacy, improved operational security, and maintained 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 on isolated events.

Unfortunately, many first- and second-generation security information and event management products do not yield sufficient network intelligence and performance attributes to more precisely identify and validate correlated events, better pinpoint attack paths, surgically remove threats, or maintain high event loads. Cisco Systems® addresses these security issues and management deficiencies with a family of scalable enterprise threat mitigation appliances. The 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, empowering companies to readily identify, manage, and eliminate network attacks and maintain compliance.

Cisco Security MARS integrates tightly with Cisco’s premier security management suite, 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, policy configuration errors, and fine-tuning defined policies.

Features and Benefits

Network Intelligent Event Aggregation and Performance Processing

Cisco Security MARS obtains network intelligence by understanding the topology and device configurations from routers, switches, and firewalls, 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 it to model packet flows through your network. Since the appliance does not operate inline and makes minimal use of existing software agents, there is little impact on network or system performance.

The appliance 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, 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, that 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 unprecedented data reduction, and compresses this information for archive. 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 system. All database functions and tuning are transparent to the user. Onboard storage and continual compression of historical data archives to network file system (NFS) secondary storage devices makes Cisco Security MARS a reliable security log aggregation solution.

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 comprises 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 mandatory access conrol (MAC) address. This automated process is accomplished by analyzing device logs such as firewalls and intrusion prevention applications, third-party vulnerability assessment data, and through 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 the Cisco Security Monitoring, Analysis, and Response System, operators have a rapid means to understand all of the components involved within an attack, down to the offending and compromised system MAC address. Cisco AutoMitigate capabilities identify available “choke-point” 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 streamlines the conventional security workflow, providing automated case assignment, investigation, escalation, notification, and annotation for daily operations and specialized audits. It can graphically replay attacks and retrieve stored event data to analyze previous events. The system fully supports ad-hoc 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 Sarbanes-Oxley, the 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, and the EU's Revised Basel Capital Framework (Basel II). 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.

Network Admission Control Support

Cisco Security MARS will parse, normalize, correlate, and report on 802.1x authentication events from both Layer 2 switches and Cisco Secure Access Control Server (ACS). Cisco Security MARS will do the same using the Extensible Authentication Protocol (EAP) protocol for Layer 3 routers and for Cisco VPN 3000 Series concentrators. This allows customers to troubleshoot device authentication methods by determining the chain of connections between the switch, the Cisco Secure ACS, the endpoint being validated, and the external authentication source, such as Active Directory or network information service (NIS). Cisco Security MARS also provides centralized reporting for Network Admission Control (NAC) Phase 1 and Phase 2 parameters that highlight the reason for device and posture authentication failure. Examples of such reports include:

- User report
- User detail
- Endpoint detail
- Rejected endpoints report
- Endpoint status queries failure report
- Application posture token distribution report
- Top ten endpoints and top ten user violations report
- Remediation time by endpoint report

Rapid Deployment and Scalable Management

Cisco Security MARS is placed on a TCP/IP 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 the Cisco Security Monitoring, Analysis, and Response System. Simply configure your log sources to point to the appliance and define any network and source through the Web-based GUI. Rapidly deploy Cisco Security MARS by

forwarding messages from existing syslog-ng or Kiwi syslog servers. This feature eliminates many network and device changes required to insert Cisco Security MARS into an operational network.

Cisco Security MARS appliance is centrally managed through a secure Web-based interface that supports role-based administration and authentication. The optional Global Controller appliance centralizes expansive security operations to provide a single view of the entire enterprise and to disseminate access privileges, configurations, updates, customized rules, and report templates, as well as to coordinate complex investigations with accelerated queries and reports that are processed locally.

As the local Cisco Security MARS appliances execute queries and rules across the enterprise, the results are efficiently consolidated for rapid and centralized analysis at the system's Global Controller. This scalable architecture yields an additional level of distributed processing and storage. The result is more cost-effective deployment and greater manageability, which addresses the requirements of large and geographically dispersed organizations.

New Features in Release 4.3.1 and 5.3.1

Login Security

This feature set is focused on improving the security of the Cisco Security MARS system when used in distributed environments. This feature set is made up of two categories of features, one that is focused on the providing secure password management and off-box authentication of Cisco Security MARS users and the second that is focused on providing session timeout control to the administrator for individual Cisco Security MARS users. Off-MARS authentication is provided via RADIUS support in Cisco Security MARS and allows Cisco Security MARS to authenticate with a RADIUS server before allowing users to login to the appliance. This functionality inherently provides Cisco Security MARS with additional capabilities such as the password aging and minimum password requirements such as length and type of password used, all via RADIUS. The session timeout features provide the administrator a means of enforcing policy on users who may not log out of the Cisco Security MARS device over longer periods of time, therefore if an administrator were to require a policy that stated Cisco Security MARS should log out users who are inactive for 15 minutes, this feature set can enforce that policy.

Syslog Forwarding

Syslog Forwarding support in Cisco Security MARS will allow Cisco Security MARS to forward syslog messages it receives from syslog sources to another syslog receiver. In earlier Cisco Security MARS releases support for receiving syslog messages from a syslog Relay device was added. Therefore the syslog forwarding feature set in this release enhances support for syslog within Cisco Security MARS, and allows for the insertion of Cisco Security MARS into an already established syslog architecture.

Cisco IPS 6.0 Dynamic Signature Updates

Dynamic Signature Update capability provides Cisco Security MARS with the ability to recognize events that are generated by a Cisco IPS device versions 5.x and 6.x. Beginning in release 4.3.1 and 5.3.1, Cisco Security MARS can discover the new signatures and correctly process and categorize received events that match those signatures. These updates provide event normalization and event group mapping, and they enable the Cisco Security MARS to parse Day Zero signatures from the Cisco IPS device. The downloaded update information is an XML file that contains the Cisco IPS signatures. This feature set provides improved security by way of automation and ease of use to the user.

Cisco Security Monitoring, Analysis, and Response System Technical Specifications

Versioning information

The 4.x releases will continue to support the MARS-20R, MARS-20, MARS-50, MARS-100e, MARS-100, MARS-200, MARS-GCm, MARS-GC appliances. The 5.x releases will continue to support features on new appliance models MARS-110R, MARS-110, MARS-210, MARS-GC2 and new addition of MARS-GC2R (new Global Controller, see Table 1 for detail). There will be significant feature parity across the two releases. Even though appliance differences result in minor differences in some feature implementations, every effort is made to provide parallel, equivalent feature support. Please refer to the Gen2 Hardware release Q&A for further details.

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 Products

Cisco Part Number (Local Controller Models)	Events/ Sec[1]	NetFlows/ Sec	Storage	Rack Unit	Power
Cisco Security MARS 20R (CS-MARS-20R-K9)	50	1500	120 GB (non-RAID)	1 RU x 16 in.	300W, 120/240V autoswitch
Cisco Security MARS 20 (CS-MARS-20-K9)	500	15,000	120 GB (non-RAID)	1 RU x 16 in.	300W, 120/240V autoswitch
Cisco Security MARS 50 (CS-MARS-50-K9)	1,000	30,000	240 GB RAID 0	1 RU x 25.6 in.	300W, 120/240V autoswitch
Cisco Security MARS 100e (CS-MARS-100E-K9)	3000	75,000	750 GB RAID 10 hot-swappable	3 RU x 25.6 in.	500W dual-redundant, 120/240V autoswitch
Cisco Security MARS 100 (CS-MARS-100-K9)	5000	150,000	750 GB RAID 10 hot-swappable	3 RU x 25.6 in.	500W dual-redundant, 120/240V autoswitch
Cisco Security MARS 200 (CS-MARS-200-K9)	10,000	300,000	1,000 GB RAID 10 hot-swappable	4 RU x 25.6 in.	500W dual-redundant, 120/240V autoswitch
Cisco Security MARS 110R (CS-MARS-110R-K9)	4,500	75,000	1,500 GB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	2x 750 W dual-redundant, 120/240V autoswitch
Cisco Security MARS 110 (CS-MARS-110-K9)	7,500	150,000	1,500 GB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	2x 750 W dual-redundant, 120/240V autoswitch
Cisco Security MARS 210 (CS-MARS-210-K9)	15,000	300,000	2,000 GB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	2x 750 W dual-redundant, 120/240V autoswitch

Cisco Part Number (Global Controller Models)	LC Models Supported	Maximum Connections	Storage	Rack Unit	Power
Cisco Security MARS GCm (CS-MARS-GCm-K9)	Cisco Security MARS 20/50 only	5	1 TB RAID 10 hot-swappable	4 RU x 25.6" (D); 19" (W) in.	2x 500 W dual-redundant, 120/240V autoswitch

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

Cisco Part Number (Global Controller Models)	LC Models Supported	Maximum Connections	Storage	Rack Unit	Power
Cisco Security MARS GC (CS-MARS-GC-K9)	Cisco Security MARS 20/50/100/100e/200 only	Not currently restricted	1 TB RAID 10 hot-swappable	4 RU x 25.6 in.	2x 500W dual-redundant, 120/240V autoswitch
Cisco Security MARS GC2 R (CS-MARS-GC2R-K9)	Cisco Security MARS 20/50 only	5	2 TB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	2x 750 W dual-redundant, 120/240V autoswitch
Cisco Security MARS GC2 (CS-MARS-GC2-K9)	All Cisco Security MARS	Not currently restricted	2 TB RAID 10 hot-swappable	2 RU x 27 3/4" (D); 3.44" (H); 19" (W) in.	2x 750 W 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

Topology Discovery

- Layer 3 and Layer 2 routers, switches, and firewalls
- Network IDS blades and appliances
- Manual and scheduled discovery
- Secure Shell (SSH), 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 via 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 seperated vector (CSV) export
- Live, batch, template, and e-mail forwarding reporting system
- Easy to use query structure built for an effective drill down to the information in a specific incident

Administration

- Web interface (HTTPS); roles-based administration with defined privileges
- Global Controller hierarchical management of multiple Cisco Security Monitoring, Analysis, and Reporting Systems
- Automated, verified updates, including device support, new rules, and features
- Continuous compressed raw data and incident archive to offline NFS storage

Device Support

- Network: Cisco IOS Software; Cisco Catalyst® OS; Cisco NetFlow; and Extreme Extremeware
- Firewall/VPN: Cisco ASA Software; Cisco PIX® Security Appliance; Cisco IOS Firewall; Cisco Firewall Services Module (FWSM); Cisco VPN 3000 Concentrator; 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; NetScreen IDP; OS; and Symantec ManHunt
- Vulnerability assessment: eEye REM, Qualys QualysGuard, and McAfee FoundStone FoundScan
- 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 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; and Network Appliance NetCache, ISS Site Protector
- Universal device support to aggregate and monitor any application syslog
- Support 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 version 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

Product Name	Part Number
Cisco Security MARS 20R	CS-MARS-20R-K9
Cisco Security MARS 20	CS-MARS-20-K9
Cisco Security MARS 50	CS-MARS-50-K9
Cisco Security MARS 100e	CS-MARS-100E-K9
Cisco Security MARS 100	CS-MARS-100-K9
Cisco Security MARS 200	CS-MARS-200-K9
Cisco Security MARS 110R	CS-MARS-110R-K9
Cisco Security MARS 110R Upgrade License to CS-MARS-110-K9	CS-MARS-110-LIC-K9=
Cisco Security MARS 110	CS-MARS-110-K9
Cisco Security MARS 210	CS-MARS-210-K9
Cisco Security MARS GCm	CS-MARS-GCm-K9
Cisco Security MARS GC	CS-MARS-GC-K9
Cisco Security MARS GC2R	CS-MARS-GC2R-K9
Cisco Security MARS GC2R upgrade license to CS-MARS-GC2-K9	CS-MARS-GC2-LIC-K9=
Cisco Security MARS GC2	CS-MARS-GC2-K9

Service and Support

Cisco offers a wide range of services programs to accelerate customer success. These innovative services programs are delivered through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see Cisco Technical Support Services or Cisco Advanced Services.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 C78-386254-06 12/07

