

# Cisco Info Center for Security Management Release 1.0

## *Integrated, Multiservice, Multivendor Security Management*

Cisco® Info Center for Security Management extends the Cisco Info Center operational management environment to offer integrated and proactive security monitoring from a central network-operations-center (NOC) and security-operations-center (SOC) facility. Management across all network operational activities, including security breaches, provides the most accurate real-time analysis of potential impact prior to the actual attack.

### End-to-End Operations Management Through a Single Management Console

The Cisco Info Center for Security Management solution provides for the collection, consolidation, and analysis of the data generated across all Cisco security tools. Based on the Cisco Info Center application, the Cisco Info Center for Security Management solution can correlate disparate events to a single breach, provide a single real-time event management interface, automatically notify personnel of potential breaches, and offer historical security reports for ongoing analysis.

Cisco Info Center for Security Management enables rapid operator responsiveness by offering several new ways to view, assimilate, and remedy real-time data on security threats and the status of the IT environment. The most critical advantage that Cisco Info Center for Security Management presents is its unique ability to provide operations teams with centralized security monitoring through the following attributes:

- *Market-leading, mature technology*—Cisco Info Center for Security Management is based on the

established OEM technology partnership with Micromuse. Micromuse is the market leader in network fault management and event consolidation. It has been delivering proven and scalable service and business assurance management solutions to more than 1400 service providers and enterprises worldwide. Cisco Info Center for Security Management can collect and process thousands of events, making it an ideal solution for managing the large volume of data security.

- *Broadest management scope*—The Cisco Info Center for Security Management solution can collect data from more than 1000 different sources, including all major network management systems. It also supports customized Cisco monitoring through support of the Cisco universal collector interfaces for syslog, Simple Network Management Protocol (SNMP) traps, and others. Support for multivendor management tools and interfaces such as Windows NT event logs, firewalls, intrusion detection systems, and antivirus applications is also provided.



- *Unique, powerful threat isolation*—The Cisco Info Center for Security Management solution offers effective correlation and automated response and notification capabilities. It can consolidate multiple, disparate security events to a single potential threat and associate security breaches to service outages. Its ability to gather a wide range of information from multiple environments helps operations staff rapidly isolate the source of threats.

#### “Manager of Managers” Streamlining Event Management

The Cisco Info Center for Security Management solution collects disparate network and security events and can consolidate and correlate multiple events to a single breach. It looks at events across the entire network and identifies network and service outages that can occur via its correlation and analysis intelligence.

The Cisco Info Center for Security Management solution can automatically notify security operations personnel of potential breaches and events via e-mail or pager based on the severity of the event. Its correlation and notification capabilities make it easier for security operations teams to focus and resolve security-related problems. The Cisco Info Center for Security Management solution supports:

- Check Point FireWall-1, Cisco PIX<sup>®</sup> Firewall, and NetScreen firewall
- Authentication and authorization from system log files, including UNIX syslog and the Windows NT Event Log
- Hardware virtual-private-network (VPN) devices, Network Address Translation (NAT), and IP Security (IPSec)
- Intrusion detection and network surveillance systems (host-based intrusion detection systems [HIDSs] and network intrusion detection systems [NIDSs])
- Network intrusion detection, utilization, protocol decodes, and network performance from Network Associates’ Sniffer Distributed
- Environmental and physical security systems from Johnson Controls Cardkey division
- All existing Cisco Info Center probes and monitors

#### Cisco Info Center for Security Management Subscriber Identity Module Tools

The Cisco Info Center for Security Management solution allows you to give your security staff a single interface to access all security information and their tools. The features in Version 1.0 allow full management control and extensible methods for locating and tracking security information that could potentially threaten IT systems and business processes. It offers policies and new tools for more effective monitoring and tracking of security data. The features include:

- *Search in Network*—You can view all events with an IP address that matches user-defined parameters.
- *Generate threat fingerprint*—You can view a graphical fingerprint of all threat events.
- *Associated Events*—You can view security events associated with a particular threat event.
- *Clear Associated Events*—This feature clears all events associated with a selected threat event from the view.
- *Change score*—You can change the score of the threat event in the view.
- *Find other end*—You can view all events associated with the currently selected threat event.

The Cisco Info Center for Security Management solution eliminates event “noise,” allowing security staff to focus on the relevant information. Cisco Info Center for Security Management can remotely collect and monitor data and bring it back to the consolidation point securely.



### **Alarm Correlation**

The Cisco Info Center for Security Management solution performs correlation by linking security events with other Cisco Info Center-collected intelligence and establishes a relationship between security events and potential incidents. Cisco Info Center for Security Management can consolidate multiple, disparate security events to a single potential threat and can relate potential security events to known service outages. Customers can easily customize and expand correlation capabilities.

### **Alarm Notification**

The Cisco Info Center for Security Management solution can also automatically notify IT and security teams and operations personnel of alarms and breaches. This functionality is completely customizable—providing initial notification on critical events and then customizing to escalate notification based upon the time and severity of the threat. Cisco Info Center for Security Management can identify ongoing critical threats and initiate threat resolutions. Customizations can be made to invoke a denial of access to any offending IP address or start a failover to a nonaffected server or services.

### **Real-Time and Historical Reporting**

The Cisco Info Center for Security Management solution is not just data consolidation and correlation. It offers intuitive, off-the-shelf reports that fit the needs of security operations management. Cisco Info Center for Security Management historically logs all the information it collects, and provides reports that can be dynamically published and distributed. Some of the reports include:

- Number of attacks by source
- Number of attacks by destination
- Threats and correlated events
- Firewall policy and Cisco IOS<sup>®</sup> configuration changes
- Top ten intruders
- Denial of service
- Top ten attack signatures
- Authorization and access summary
- Alarm generation summary
- Attack signatures summary

The Cisco Info Center for Security Management can be sold independently or as an add-on extension package to Cisco Info Center customers. The Cisco Info Center for Security Management Policy Pack provides customizations and automations for the Cisco Info Center Info Server, Cisco Info Center for Security Management Impact, Cisco Info Center Reporter Gateway, and Cisco Info Center Info Mediator.

## Third-Party Integration Support

- Asita Technologies' Asita Security Operating System (Asita SOS) supporting Asita's LS100 GS GS2 line
- Johnson Controls Cardkey solutions
- NetScreen's GlobalPRO

- Network Associates' Sniffer Distributed
- NIKSUN NetDetector

## Platform Support

- Sun Solaris 8.0 or earlier



Corporate 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: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

Asia Pacific Headquarters  
Cisco Systems, Inc.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe