

CiscoWorks Security Information Management Solution

Q. Q. What is CiscoWorks Security Information Management Solution?

A. CiscoWorks Security Information Management Solution (CiscoWorks SIMS) is a solution that collects and analyzes security event information from across the enterprise, letting you detect and respond to security events as they occur. With CiscoWorks SIMS, you can manage your growing security device infrastructure without increasing the size of your existing security staff.

CiscoWorks SIMS delivers:

- Complete event monitoring for SAFE and multivendor security environments
- Real-time event correlation to detect both known and unknown threats
- Advanced visualization for fast and intuitive security monitoring
- Integrated risk assessment to understand the overall vulnerability of any particular asset within the enterprise
- Comprehensive reporting and forensics for all levels of security operations and management

CiscoWorks SIMS delivers these capabilities using the award-winning netForensics v3.1 software. netForensics v3.1 automates many of today's security analysis and reporting tasks. With real-time drill-down capabilities, advanced correlation, visualization, and reporting, netForensics v3.1 lets you access critical security information from any Web browser. The

highly scalable, distributed architecture of netForensics v3.1 makes this a high-performance security solution, scalable for enterprises of all sizes.

Q. What is security information management?

A. Security information management (SIM) technology collects, analyzes, and correlates security device information from across the enterprise in a series of four phases: normalization, aggregation, correlation, and visualization. In the normalization and aggregation phases, security events are collected from virtually all intrusion detection systems (IDSs), firewalls, operating systems, applications, and anti-virus systems, and transformed into one simple, easy-to-understand Extensible Markup Language (XML) format. Formatted records are then correlated using two powerful correlation engines, which rely upon statistical and optional rules-based correlation technologies. Finally, netForensics v3.1 displays correlated results on a centralized, real-time console with a graphical, Java-based interface that is powerful, intuitive, and user-friendly.

Q. What is the relationship between Cisco and netForensics?

A. Cisco has a historical relationship with netForensics that includes financial investment in netForensics, joint engineering, technical support, sales, marketing, and training.



Q. How is CiscoWorks SIMS sold?

A. CiscoWorks SIMS (including netForensics v3.1) is available for ordering using the following options:

1. Starter Pack on Solaris (includes licenses to monitor 30 devices, one master engine, one distributed engine, one Oracle database, and agent software)
2. Starter Pack on Linux (includes licenses to monitor 30 devices, one master engine, one distributed engine, one Oracle database, and agent software)
3. License for monitoring 20 additional devices
4. License for one additional distributed engine
5. License for one additional Oracle database on Solaris
6. License for one additional Oracle database on Linux

The part numbers are listed in the CiscoWorks SIMS data sheet. An option that delivers an appliance with CiscoWorks SIMS preinstalled on a hardware server with Linux may be available in the future. Please monitor the CiscoWorks SIMS data sheet at Cisco.com for future availability of this option.

netForensics has additional options not listed above. These options can be purchased directly from netForensics.

Q. What are normalization, aggregation, correlation, and visualization?

A. *Normalization:* More than 20,000 different event types are produced by today's perimeter security devices. Through netForensics v3.1 agent technology, these event types are mapped into as few as 100 netForensics XML-based alarm IDs—significantly reducing the burden of security data analysis.

Aggregation: Event aggregation is a process of de-duplication that reduces large volumes of event data into a manageable set. This is especially useful for events such as ping sweeps or port scans, where similar events are reported multiple times by firewall devices. Event aggregation is also used to de-duplicate alerts from multiple IDS devices.

Correlation: Formatted records are correlated using two distinct yet complementary forms of event correlation—the first is a statistical correlation mechanism which relies upon event categorization and threat scoring to determine the threat potential of security based anomalies. The second is an optional rules-based correlation feature that separates “false-positive” security alarms from potentially significant security incidents by invoking “time-aware” security policy rules for each event received.

With statistical correlation, normalized security events are categorized into security incident types by asset or asset group. For each asset, a threat score is continuously computed by combining event severity with the asset value to determine an overall measurement of security incident potential. The primary advantage is the ability to find anomalies that may go undetected by a rules-based correlation implementation.

Both of these correlation technologies are highly accurate, and simple and straightforward to implement. Each approaches event correlation from a different perspective, protecting enterprises from a broader range of potential security incidents. netForensics v3.1 provides a comprehensive correlation solution that is integral to the overall suite of SIM capabilities.

Visualization: With netForensics v3.1, security professionals use a single, real-time, Java-based console that centrally detects and responds to security events across the enterprise as they occur—resolving security threats before they become a problem.



Q. What does the netForensics v3.1 architecture entail?

A. netForensics v3.1 features an innovative architecture for comprehensive SIM. Elements of this architecture include:

- netForensics v3.1 agents—Collect data from disparate, multivendor security technologies and applications; then transform vendor-specific formats into normalized XML data and forward this information to the netForensics v3.1 engines.
- netForensics v3.1 engines—Collect, filter, analyze, and categorize normalized data fed by the agent; with multiple, parallel-engine capabilities, netForensics v3.1 ensures unlimited scalable operations for any network size or growth, and adds inherently growth-tolerant operations from this distributed architecture.
- Forensics data repository—Consolidated, normalized historical data is automatically maintained in the netForensics v3.1 data repository; maintained in an Oracle database, customers can use existing industry-standard reporting, query, and business intelligence tools for analysis or reporting, in addition to the default netForensics v3.1 report and analysis. This trove of data is invaluable for researching past problems, identifying and tracking trends, and heuristic operations to continually improve security effectiveness.

Q. Does netForensics v3.1 replace our current security technology?

A. No. netForensics v3.1 works in concert with your existing security infrastructure to gather, analyze, and correlate the vast amount of security event information that is produced by today's security devices. In the event of a breach, netForensics lets operators and analysts quickly determine the source of virtually any security threat.

More importantly, netForensics lets companies take control of enterprise security management by increasing the capacity and effectiveness of their existing security teams. With netForensics, you can manage your growing security device infrastructure without increasing the size of your existing security staff.

Q. Don't existing security technologies already detect and trap security problems in real time?

A. Many of today's security attacks occur across an entire enterprise (denial of service attacks, for example). Additional technology is needed to collect the security event information that occurs at the enterprise endpoints, and to correlate that information to determine whether an attack is occurring across the network infrastructure. netForensics can detect incidents that are not isolated to one IDS or firewall, but are spread across multiple systems within the infrastructure.

Q. Can you really detect and prevent all security incidents in real time?

A. Given the myriad of attack techniques, the huge numbers of potential attackers, and the rapid pace of innovation of security threats, no technology can detect and prevent all problems. However, netForensics v3.1 gives you the technology edge you need to detect numerous security incidents—many more than what is capable by a few isolated devices.

netForensics gives security teams the ability to immediately detect suspicious activities and investigate them further. In most instances, netForensics will have already identified the specific attack, allowing operators to take appropriate action to either eliminate or minimize damage.



Q. Tell me about the netForensics v3.1 Interface.

A. With netForensics v3.1, a single real-time, Web-based console lets you centrally detect and respond to security events across your enterprise as they occur—so security threats are resolved before they become a problem. Your security team can identify and respond to more threats, more effectively, without adding more staff. The real-time console receives its information from the master engine, which performs high-level aggregation and correlation for multiengine installations and then passes real-time data streams to the real-time console (RTC).

The RTC is written in pure Java so that robust functions can be carried out at the client level. Yet, while the RTC is functionally rich, it interoperates with a dedicated Web server to perform many tasks. This enables the RTC to be robust yet lightweight.

Using netForensics v3.1 visualization capabilities, operators, analysts, and managers can garner the information necessary to determine overall threat posture, and to investigate and respond to individual attacks before they create damaging effects within your enterprise. netForensics v3.1 offers a series of intuitive real-time interfaces combined with in-depth reporting and historical analysis to help understand threats and respond to security attacks, including:

- The dashboard view provides a real-time, enterprise-level view of security trends
- The netForensics v3.1 RTC facilitates fast isolation of security attacks using real-time correlation and drill-down capabilities
- SIM reports provide comprehensive risk and threat trend analysis

Q. What makes Cisco a leader in this market?

A. While there are several information security vendors in today's marketplace, CiscoWorks SIMS is based on award-winning technology. Network Computing Magazine awarded netForensics with both the Editor's Choice and Well-Connected awards at last year's Networld + Interop Tradeshow.

Q. How does netForensics v3.1 work with enterprise management solutions such as HP Openview and Micromuse?

A. netForensics v3.1 can send information on security events to enterprise management consoles, including MicroMuse Netcool and HP Openview. netForensics v3.1 offers several options when configuring enterprise management security support, and can also be used to automatically open trouble tickets in help desk systems based on administrator-defined rules.

netForensics v3.1 focuses solely on comprehensive SIM. The power of netForensics v3.1 lies in its ability to understand the security message in its entirety, and provide information on all security events. These capabilities make netForensics v3.1 an excellent complement to enterprise management solutions. By integrating netForensics v3.1 with MicroMuse Netcool or HP Openview, enterprise management can focus on security.

Q. What security devices does netForensics v3.1 support?

A. netForensics v3.1 is a fully scalable, three-tier architecture that allows for deployment in a single location with limited device support, or globally throughout an ever-growing distributed environment.

It provides two kinds of device support:

1. Native integration—Native agents are consistently being added to the netForensics v3.1 architecture. These include Cisco devices, Check Point Firewall, ISS IDS, Entcept HIDS, Cisco access control lists (ACLs) and virtual private networks (VPNs), Windows NT and UNIX logs, and Snort and Dragon sensors.

2. Universal Agent integration—It is critical to incorporate an increasingly complex and wide array of devices, applications, and custom data into its real-time intelligence engines and repository. netForensics v3.1 provides an industry-standard set of XML utilities, making up the Universal Agent, and harnessing a virtually unlimited set of security information into its architecture.

The underlying architecture is secure and reliable XML over TCP. It is shipped with a set of self-health management utilities that further reduce the need for added system and database administration requirements.

Q. What is risk assessment?

A. Risk assessment is a compound of threat, vulnerability, and value. Since vulnerabilities are weaknesses that allow threats to happen, the vulnerability of an asset can be estimated by evaluating its *popularity* and *exposure*. The popularity of an asset is a measure of its availability as a target (number of accesses to a Web server), while its exposure is a measure of its function (the number of open ports and the nature of the listening network services). While the value of an asset is subjective, the enterprise administrator can still

make relative estimates of all assets being managed. In netForensics v3.1 the value, popularity, and exposure for an asset are explicitly defined by the administrator and used for quantitative risk assessment.

Q. What is risk management?

A. Risk management is a continuous process of assessing threats across the enterprise and ensuring that the risk posed by these threats is within acceptable levels. According to the SANS Institute, risk is comprised of threat, value, and vulnerability. Threats are activities that represent possible danger to the network assets. The value of network assets, and the information they contain, are subjective and can vary over time. Value is usually defined by the role the system plays within the company, and the data stored or processed by the system. Vulnerabilities are system and software weaknesses that allow threats to inflict damage.

netForensics v3.1 provides threat and risk assessment for the enterprise using proprietary formulas that calculate threat and risk scores based on event netForensics severity counts, asset value, popularity, and exposure, and intruder threat factor and frequency.



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

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

All contents are Copyright © 1992-2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, Aironet, Catalyst, and Cisco IOS are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
(0303R) 203051/ETMG_04/03