



# Symantec™ Incident Manager

*Real-time security incident management for enterprise network environments*

## > Complex threats require an integrated management solution

Network attacks, blended threats, and internal abuse regularly compromise critical information systems, usurp bandwidth, and lead to loss of sensitive corporate data. Enterprises have responded by deploying a combination of security products and services, such as virus protection, firewalls, and intrusion detection from multiple vendors.

Security administrators rely on the data generated by these point products to identify and respond to critical incidents, such as attacks, virus outbreaks, or system vulnerabilities. However, the data generated are disjointed and suboptimal, and the amount of data is overwhelming for resource-constrained security personnel who must quickly identify incidents requiring an immediate response. Adding to the problem, lack of centralized management of these disparate products prevents security personnel from gaining a unified view of the data.

Administrators need a comprehensive view of the company's overall risk exposure, a way to measure the effectiveness of existing security investments, and a means to effectively manage security incidents.

## > Real-time security management

Symantec™ Incident Manager correlates security messages in real-time from disparate products across the enterprise to identify and prioritize security incidents. It connects security knowledge to action by coordinating and tracking response activities throughout the incident lifecycle helping enterprises respond quickly and effectively, thereby minimizing the business impact of information security breaches. Symantec Incident Manager is built on Symantec Enterprise Security Architecture (SESA), a standards-based infrastructure that enables Symantec and third-party security solutions to work together to provide secure, manageable, and scalable enterprise security.

Symantec Incident Manager allows enterprises to transform security data into prioritized, actionable intelligence, thus reducing costs and minimizing risk. Advanced features enable incident identification, complete tracking through the incident lifecycle, and dynamic prioritization of incidents and actions. The solution also provides expert guidance supported by SANS and CERT best practices.

This solution simplifies information security management and enables enterprises to:

- Identify incidents through analysis and correlation of event traffic
- Prioritize responses to identified incidents
- Track incidents to effective resolution
- Document the actions taken, to preserve a record of the incident for audit, legal, and process improvement purposes

## KEY POINTS

- > **NEW!** Powerful, automated, near real-time correlation engine transforms security data into actionable intelligence, enabling rapid response to complex security threats
- > Results in fewer undetected attacks and reduced monitoring costs
- > **NEW!** Correlates attacks with the presence or absence of vulnerabilities on targeted systems, reducing false positives
- > Reduces monitoring costs since staff spend less time responding to false positives
- > Enables staff to respond to genuine threats and frees them to focus on higher-value strategic initiatives
- > Fosters quicker containment and reduces incident impact
- > Sets incident priorities dynamically, based on severity of business impact, improving decision making and resource allocation
- > Tracks incident handling activities from identification to closure, keeping the focus on corrective action
- > Provides dynamic, expert guidance based on SANS and CERT incident response best-practices framework, promoting complete and consistent responses to every incident
- > Records and reports on key metrics, enabling enterprises to visualize and refine the effectiveness of security processes
- > Works with customers' existing security products, maximizing the value of existing security investments

## > Features and benefits

The following features of Symantec Incident Manager enable a more efficient, traceable, and measurable, incident response:

- **Correlation and incident identification** Symantec Incident Manager embeds correlation and analysis technologies to help security analysts correctly and completely identify the boundaries and characteristics of an incident. The system examines event feeds from disparate security devices across the enterprise, normalizes them and automatically identifies incidents in real time to help improve incident detection and reduce false positives. By tracking system information, providing a robust query tool, and displaying links between event signatures and safeguards, Symantec Incident Manager helps administrators understand important characteristics of each incident, reduce monitoring costs and simplify the identification process.
- **Business impact analysis** Using a sophisticated Risk Analysis Engine, Symantec Incident Manager assesses each incident's impact on an organization's business in terms of confidentiality, integrity, and availability. Each incident is rated according to the systems affected, how important each is to the overall business, and the severity of the attack or vulnerability. Organizations classify network assets using risk profiles that can be tailored to specific to different parts of their business, resulting in analysis that is relevant in a business context.
- **Dynamic prioritization** In real time, the system compares the criticality of pending resolution steps with the criticality of other incidents and continually resets priorities for incidents and actions. This allows staff to focus resources on solving the most serious problems first.
- **Incident tracking** Effective incident response requires considerable coordination between security teams and system administrators who can effect the changes required to restore vulnerable systems to an acceptable risk profile. Symantec Incident Manager tracks each incident and related response activities throughout the complete incident lifecycle. It also provides a checklist that tracks the status of all response activities across multiple events and systems to facilitate a complete and consistent response to every incident.
- **Dynamic expert guidance** Symantec Incident Manager provides guidance based on the SANS and CERT incident response framework—an acknowledged best-practices framework—to facilitate the highest level of incident handling. It works in tandem with customer-specific policy controls to help security personnel resolve the incident as quickly and effectively as possible. Guidance also helps security personnel provide clear and comprehensive instructions to the broader IT staff as they direct their activities to resolve each incident.
- **Broad device support** Symantec Incident Manager integrates with Symantec firewall, antivirus, intrusion detection, and vulnerability assessment security applications via SESA or a SESA-bridge. It also interoperates with protection applications from leading vendors, enabling integrated management across multiple vendors' products, at each level of the network (client, gateway, and server). Events from third-party products are normalized, reduced and consolidated via SESA Collectors.

- **Security intelligence** Symantec Incident Manager generates graphs and reports that provide a centralized and unified view of the enterprise's security posture and help security and IT managers answer key security management questions:
  - Which systems are under attack?
  - What is the impact to my business (in terms of confidentiality, integrity and availability)?
  - What is the nature and frequency of attacks over time?
  - Are the company's incident handling processes effectively reducing risk?
  - Is IT meeting its service-level obligations to each business unit?
  - What is the potential business impact of unresolved attacks and vulnerabilities?
- **Expert content** Security teams need accurate information to handle increasingly frequent and complex information security threats. Symantec Incident Manager includes the following:
  - Correlation rules and conclusions: Logic to detect known attacks and escalate anomalous activity or activity from suspicious sources.
  - Action recommendations: Security expertise to guide the user through the process of identifying and handling both general and specific incident types.
  - Vulnerability and safeguard data: The most current vulnerability data drawn from the Symantec vulnerability database.
  - Device-specific knowledge: Expert knowledge about security point products is used to translate device message formats and normalize device specific signatures in preparation for correlation.

## > **Backed by Symantec Security Response**

Symantec Security Response offers a range of powerful security resources, including world-class product support, and the non-stop vigilance of Symantec's industry-leading global research and technical support centers. Our intrusion experts, security engineers, and virus experts work together to provide thorough coverage around-the-clock, constantly researching viruses, malicious code, evolving vulnerabilities and exploits, and the latest intrusion techniques. In addition, Symantec Security Response is continuously at work developing automated emergency response systems that detect security problems, alert customers, and securely deliver cures to Symantec Enterprise Security customers.

For more information about Symantec Incident Manager, visit  
<http://enterprisesecurity.symantec.com>

**SECURITY MANAGEMENT TECHNOLOGY IS A KEY COMPONENT OF SYMANTEC ENTERPRISE SECURITY. SYMANTEC ENTERPRISE SECURITY COMBINES WORLD-CLASS TECHNOLOGIES, COMPREHENSIVE SERVICES, AND GLOBAL EMERGENCY RESPONSE TEAMS TO HELP BUSINESSES RUN SECURELY AND CONFIDENTLY.**

**SYSTEM REQUIREMENTS**

## SYMANTEC INCIDENT MANAGER 2.0

## SESA Foundation Components v. 1.1

*(Symantec Incident Manager uses the Symantec Enterprise Security Architecture (SESA) to provide integration and management across a wide range of leading security products. Symantec Incident Manager includes the SESA Foundation pack, a set of scalable, extensible, and secure technologies that make Symantec's Enterprise Security products interoperable and manageable. Refer to SESA Foundation Component requirements, below.)*

## IN ADDITION TO SESA FOUNDATION COMPONENT REQUIREMENTS, SYMANTEC INCIDENT MANAGER REQUIRES THE FOLLOWING:

- 30 MB disk storage space for Symantec Incident Manager program files and associated configuration data.
- 32 GB disk storage space for incident data-store data. (Estimated to contain approximately 1 month of incident data under nominal operating conditions. More storage may be required in certain environments, to archive or to keep incidents for a longer period of time.)

## SYMANTEC INCIDENT MANAGER RULES ENGINE

*The Rules Engine is included with Symantec Incident Manager and required for automatic, real-time correlation. It can be installed on the same machine as the other Symantec Incident Manager components. For improved performance, Symantec recommends installing the Rules Engine on a separate machine that meets the following minimum requirements:*

- Intel Pentium III 2.0 GHz processor
- 2 GB RAM memory
- Microsoft Windows 2000 Server or Advanced Server (with Service Pack 3 installed)
- SUN JDK/JRE 1.3.1\_02-b02
- 50 MB disk storage for program files and associated configuration data

**Console (Remote)**

- System capable of running Microsoft Internet Explorer 5.5 SP2 or 6.0
- Intel Pentium-compatible 400 MHz processor (Windows)
- ActiveX, scripting, and Java Virtual Machine (JVM) must be enabled in the Internet browser
- 256-color video adapter
- TCP/IP Communications enabled

## SESA FOUNDATION COMPONENTS

**SESA Manager**

*(with all SESA middle-ware components installed on a single system)*

- Windows 2000 Server SP2 / Windows 2000 Advanced Server SP2
- Intel Pentium-compatible 1GHz processor (Windows)
- 1 GB Memory minimum required
- 15 GB disk space (SESA DataStore and SESA Directory program files / SESA Directory data)
- 128 GB disk space per managed security product instance (maintaining 1 month of SESA DataStore security event data)
- *Disk space requirements may increase significantly depending upon the number of events received by the SESA DataStore and the length of time they are stored*
- TCP/IP Communications enabled
- Transport Layer Security (TLS) / Secure Socket Layer (SSL) Version 3.0 enabled

**SESA Agent**

- Windows NT 4.0 SP6a / Windows 2000 Server SP2 / Windows 2000 Advanced Server SP2 / Windows 2000 Professional SP2 / Windows XP
- RedHat Linux 7.2 / Solaris 7 (UltraSPARC only) / Solaris 8 (UltraSPARC only)
- Intel Pentium-compatible 133 MHz processor (Windows)
- 32 MB memory for SESA Agent
- 64 MB memory per integrating SES product
- 40 MB Disk Space (program files)
- TCP/IP Communications enabled

## INCLUDED AND SUPPORTED MIDDLEWARE COMPONENTS

The following technologies are included and/or supported, as noted, with the Symantec Enterprise Security Architecture middle-ware:

**SESA Manager**

Included and installed components

- SUN Java Development Kit (JDK) / SUN Java Runtime Environment (JRE) 1.3.1\_02-b02
- IBM Apache HTTP 1.3.19
- Tomcat 4.03
- IBM Directory Server 4.1.1
- IBM DB2 Personal Edition 7.2, FixPack 5 | Included as an optional install by SESA

Supported, but not included, components

- Existing installation of IBM DB2 Workgroup Edition 7.2, FixPack 5 on Windows 2000
- Existing installation of IBM DB2 Enterprise Edition 7.2, FixPack 5 on Windows 2000
- Existing installation of IBM DB2 Extended Enterprise Edition 7.2, FixPack 5 on Windows 2000

**SESA Agent**

- SUN Java Runtime Environment (JRE) 1.2.\_008 minimum; 1.3.1\_02-b02 recommended
- *1.3.1\_02-b02 required when co-located w/SESA manager*

**WORLD HEADQUARTERS**

20330 Stevens Creek Blvd.  
Cupertino, CA 95014 U.S.A.  
408.517.8000  
800.721.3934

For Product Information  
In the U.S., call toll-free  
800.745.6054

[www.symantec.com](http://www.symantec.com)

Symantec has worldwide operations in 38 countries. For specific country offices and contact numbers please visit our Web site.