

Symantec Enterprise Security Manager™ 6.0
Comprehensive, Policy-based Security Assessment and Management

Availability 3

What is Symantec Enterprise Security Manager? 3

Value Statements 3

Key Points..... 4

What’s New? 4

Continuing Key Features & Benefits 5

System Requirements..... 7

Licensing Symantec Enterprise Security Manager 10

Target Market..... 13

Glossary..... 15



Control Information

Date First Issued	August 12, 2003
Audience	Symantec global sales
Distribution Control	Limited initially to Symantec employees. After legal review, channel partner and customer versions will be available.
Author	Allison Fung

Availability

Following are the first customer ship dates in each region (subject to change without notice). Consult your regional marketing manager for launch dates and activities.

Region	Language	First Customer Ship
North America	English	October 27, 2003
Latin America	English	October 27, 2003
EMEA	English	November 24, 2003
AsiaPac	English	TBD
Japan	English	TBD

What is Symantec Enterprise Security Manager?

Symantec Enterprise Security Manager (ESM) rigorously evaluates computer systems and software applications against baseline security policies to ensure they are configured and patched and being used properly. In addition, Symantec ESM also finds and reports on computer systems that are not appropriately patched and could be exploited by malicious attacks. By using Symantec ESM, companies can avoid many costly security problems by ensuring their systems are compliant with stringent usage standards and that systems not patched according to policy are discovered and promptly fixed.

Value Statements

CxO

Symantec Enterprise Security Manager (ESM) makes it easier to comply with mounting government and industry information privacy regulations in order to avoid regulatory fines, and to prevent loss of shareholder value by protecting against security breaches. ESM does this by measuring whether computer systems and applications are being used according to your defined corporate security policies and standards. By proactively identifying systems that are in non-compliance, companies can remedy problems before they become costly.

CIO/CISO/IT Director

Symantec Enterprise Security Manager (ESM) automatically assesses critical business delivery systems (servers, applications, networks and security controls) for policy compliance, including patch compliance needed to eliminate many vulnerabilities. This allows your organization to:

- Better understand your security and risk posture
- Better plan and prioritize future security spending

- Use security headcount more effectively.

Symantec ESM covers critical enterprise IT infrastructure with lower hardware and manpower requirements. This means improved security insight without increased spending.

Key Points

- Provides centralized, automated and comprehensive security analysis of mission critical e-business applications and operating systems, using well over 2,000 security checks designed to prevent exploitable vulnerabilities by ensuring systems are being used according to standards and patched according to policy.
- Uses intelligent agents designed specifically for UNIX, Windows®, NetWare®, Linux, VMS and IBM® iSeries™ AS/400® as well as for Web and Database applications to perform assessments fast and accurately and without disruption to IT operations.
- Provides comprehensive management reports and security recommendations.
- Backed by Symantec™ Security Response, the world's leading Internet security research and response organization.

What's New?

New Platform Support

Symantec ESM 6.0 adds Microsoft® Windows 2003 for Intel® servers and IBM iSeries (AS/400) support to the large list of currently supported operating systems. New in this release is native support for Oracle® and IBM DB2® relational databases, as well as Microsoft Internet Information Server, Sun Microsystem SunONE™ (previously known as iPlanet™), and the Apache™ Web servers.

Pre-configured Security Policies

Organizations can now holistically manage and measure compliance to the company security policy, or to one of the pre-defined security policies in operating systems and applications from a central location.

With Symantec ESM 6.0, the following modules are now available as a complete out-of-the-box solution:

- Policy compliance modules and sample baseline standards-based security policies for market leading Web server and database application platforms.
- Policy compliance modules and sample baseline standards-based security policies for market leading firewalls.



- Policy compliance assessment for popular industry security standards and regulations, including: ISO I7799, HIPPA, Sans Top 20, and the Center of Internet Security (CIS).

Integration with SESA™

Symantec ESM 6.0 includes new transition and integration tools supporting Symantec™ Enterprise Security Architecture (SESA). Symantec ESM security data can be utilized by Symantec™ Security Management System components, such as Symantec™ Incident Manager, thereby delivering even greater value to your investment.

Continuing Key Features & Benefits

Comprehensive, Policy-Based Assessment

- Collects and correlates the security assessment data into a single, enterprise-wide series of reports that allow you to quickly identify non-compliant systems.
- Includes an automated 7x24 scheduler, making it easy to consistently perform routine security assessments.

Powerful, Enterprise-wide Management

Centralized Administrator Console

Provides a centralized console that allows you to view the security assessment data of up to 10,000 systems from a single location—for a quicker, more thorough analysis (or “health check”) of your enterprise.

Centralized Deployment

Allows you to remotely, locally, or silently deploy new/updated Symantec ESM software to Agents from a central console—saving the time and cost of traveling from machine to machine and making it easier to ensure that all systems have the most up-to-date protection.

Centralized Reporting

Offers powerful, centralized reporting to quickly identify non-compliant systems from inside the enterprise and from the Internet.

With Crystal Reports® integration, Symantec ESM provides the appropriate level of detail to meet varying business needs, giving you:

- A comprehensive view of the state of your security enterprise-wide
- The ability to drill down to analyze individual problems on individual systems



- 40 pre-defined reports—making it easier to view the information you need. Reports include:
 - All systems with a specified vulnerability
 - Executive summary reports
 - Detailed reports per agent
- The option to save, export, print, and email reports, so you can easily distribute them throughout the organization.
- The ability to customize reports or create completely new reports to meet the specific business needs of your organization—for added flexibility.

Delegation of Security Tasks

Allows you to separate and delegate security administrative tasks to specified individuals—distributing and, thus, easing administrative burden.

Scalable Enterprise Architecture

- Offers a unique, three-tier architecture that allows Symantec ESM to run in parallel across all systems—for faster system-wide assessment:
 - *Host-based Agents*, which run on each server and desktop, audit all areas of a system or application for vulnerabilities and deviations from the corporate security policy and report them to Managers.
 - *Managers*, which reside throughout your network, collect the vulnerabilities and deviations from the Agents, consolidate them, and report them to the Symantec central security console.
 - *Administrator console*, which runs on an individual desktop or in a Network Operations Center and provides centralized management across your enterprise.
- Uses minimal network bandwidth as all security assessments occur on each agent system with only secure, encrypted, non-compliance information traveling across the network.
- Scales easily—from smaller installations to very large installations that require support for thousands of systems running a variety of operating systems—to meet the expanding needs of your enterprise.

LiveUpdate™

- Allows you to download new Security Updates from the Internet and deploy them enterprise-wide through the Symantec ESM console—to provide up-to-date



protection and reducing cost of ownership. (Symantec ESM Security Updates are available to Symantec ESM users with current maintenance agreements.)

- Lets you configure Symantec ESM Agents to receive Security Updates via LiveUpdate from a single manager, a group of managers, or not to accept the Security Updates at all—to fit your security policy settings.

Relational Database Support

- Allows you to store Symantec ESM data in Oracle, SQL Server, and Microsoft® Access databases, using a secure database uplink application—for more efficient ties to your back office processes.
- Lets you further analyze this data, using the new reporting console to create custom reports that suit your organization's needs.

Security Policy Import/Export Utility

Lets you:

- Export your company security policies to disk and save them for backup purposes, allowing you to quickly restore them without productivity loss should they become corrupted or accidentally changed.
- Distribute company security policies via email to remote Symantec ESM Managers where they can be imported and used immediately, saving administrator time/resources and ensuring consistent policies enterprise-wide.

System Requirements

Console

- Microsoft Windows NT 4.0 Server/Workstation service pack 5.0 or higher
- Windows 2000 Professional, Server or Advanced Server service pack 1.0 and higher
- Windows XP Professional; Windows ME/98

Manager

Microsoft Windows

- Windows NT 4.0 server/workstation service pack 5.0 or higher
- Windows 2000 professional, server or advanced server service pack 1.0 and higher
- Windows 2003 Server

UNIX

- HP-UX[®] v10.20 – v11i
- Sun Solaris[™] v2.5.1 – 2.8
- IBM AIX v4.3.1- 5.2

Server OS Agent

Servers Running Microsoft Windows

- Windows NT 4.0 Server/Workstation service pack 5.0 or higher
- Window 2003 Server
- Windows 2000 Professional, Server or Advanced Server service pack 1.0 and higher
- Windows XP professional, Windows 2003 Server

Servers Running UNIX / Linux

- HP-UX v10.20 - 11i
- Sun Solaris v2.5.1 - 2.9
- IBM AIX[®] v4.3.1- 5.2
- Red Hat[®] Linux v7.1 – 7.3
- Compaq[®] Tru64 v.4.0-5.1
- SGI Irix[®] v6.3+

Servers Running Novell NetWare

NetWare v4.x - 6.x

Digital VMS Midrange

OpenVMS (Alpha processor) v7.2, 7.3

IBM AS/400 Mid-range

IBM iSeries (OS/400); V5R1M0, V5R2M0

Web Server Application

- IIS on Windows
- SunONE on Solaris
- Apache on Linux

Database Application

Oracle 7

- Oracle 7.3.4 on Solaris 2.6-8
 - Oracle 7.3.4 on HP-UX 10.20-11i
 - Oracle 7.3.4 on AIX 4.33+
-

Oracle 8, 8i

- Oracle 8.0.x on Solaris 2.6-8
 - Oracle 8.0.x on HP-UX 10.20-11i
 - Oracle 8.0.x on AIX 4.33+
 - Oracle 8i on Solaris 2.6-8
 - Oracle 8i on HP-UX 10.20-11i
 - Oracle 8i on AIX 4.33+
-

Oracle 9i, 9.2

- Oracle 9i on Solaris 2.6-8
 - Oracle 9i on HP-UX 10.20-11i
 - Oracle 9i on AIX 4.33+
 - Oracle 9.2
-

IBM DB2

IBM DB2 UDB 7.2 on Windows (See supported Windows versions under “Servers Running Microsoft Windows”)

Standards and Regulations Policy

- ISO17799, HIPAA
- SANS Top 20 for Windows UNIX and Linux
- CIS Benchmark for Solaris

Licensing Symantec Enterprise Security Manager

License Program

ESM will be sold under all three Value programs (Value, Academic and Government) and Elite (Forecast and Commit) discount programs.

License Options (US/CANADA):

- Media Pack
- License (Managers, agents, additional CPUs)
- Upgrade / Competitive Upgrade License
- Gold Maintenance (1 year, 2 year, renewal)
- Platinum Maintenance Uplift (1 year, 2 year, renewal)

What Do Customers License?

Customers must license the following Symantec ESM components:

- **Agents**—which are installed on each server and desktop. Agents audit all areas of a system or application for vulnerabilities and deviations from the corporate security policy and report them to Managers.
- **Managers**—which store and enforce the licenses. Managers reside throughout your network, collecting the vulnerabilities and deviations from the Agents, consolidating them, and reporting them to the Symantec centralized console.

The Windows NT/2000/Me Administrator console is free and requires no license key.

Deliverables

When customers purchase Symantec ESM, they receive:

- A Media Pack, which includes all Symantec ESM Console, Manager, and Agent software for all supported platforms, as well as soft copies of the Symantec ESM User Manual, Installation Manual, and Release Notes
- Hard copies of the Symantec ESM User Manual, Installation Manual, Release Notes, and an errata sheet
- A License Certificate with serial number (needed to obtain a license key)

License Keys

The software licenses for the Manager and Agent components are enforced through license keys installed at the Managers.



To generate a permanent license key, customers must provide:

- The number of Agents that can register to the Managers (recommended limit is 2000 per Manager)
- The machine names (or network address) of the Managers

By incorporating these elements into each license key, the license becomes tied to a specific machine and will not support more Agents than have been purchased.

NOTE: A short-life, evaluation license key can be created for customer trial purposes. Walkaround licenses are available for authorized consultants and auditors (not available through the channel) and require regional manager authorization.

Licensing Scenarios

Example #1

An organization wishes to purchase ESM and deploy it at its two main offices. ESM will be installed on a total of 200 Windows NT/2000 servers, 100 UNIX servers, 10 Linux servers, 100 UNIX/Windows Workstations, 5 NetWare servers, 1 VMS server and 2 IBM iSeries (OS/390) platforms. The agents will be controlled by two ESM managers (a UNIX manager at site A and a Windows 2000 Server Manager with a single CPU at site B). ESM will be administered through 4 Windows XP Consoles. In addition, they have 6 Oracle 9i database servers running on the UNIX servers above.

Description	Qty
Symantec Enterprise Security Manager 6.0 Media Kit	2
Symantec Enterprise Security Manager 6.0 Server Manager Lic	2
Symantec Enterprise Security Manager 6.0 Server Agent Windows Lic	200
Symantec Enterprise Security Manager 6.0 Server Agent Unix Lic	100
Symantec Enterprise Security Manager 6.0 Server Agent Linux Lic	10
Symantec Enterprise Security Manager 6.0 Server Agent NetWare Lic	5
Symantec Enterprise Security Manager 6.0 Server Agent VMS Lic	1
Symantec Enterprise Security Manager 6.0 Server Agent iSeries Lic	2
Symantec Enterprise Security Manager 6.0 Workstation Agent Lic	100

*Note: ESM consoles are included at no additional cost. There is no additional charge for the Oracle 9i database servers since they are hosted on the UNIX servers and the application modules are now included in ESM 6.0.

Example #2

An organization wishes to purchase an additional 20 ESM Windows 2000 Server agents and 2 new media kits (which include the CDs and documentation). In addition, they



would like to trade in 40 licenses of a competitor’s products for 40 more ESM agents on Windows. This customer also has 4 Web servers running on new Linux servers that they need to secure. They would also like Gold Maintenance on all agents and managers.

Description	Qty
Symantec Enterprise Security Manager 6.0 Media Kit	2
Symantec Enterprise Security Manager 6.0 Server Agent Windows Lic	20
Symantec Enterprise Security Manager 6.0 Server Agent Linux	4
Symantec Enterprise Security Manager 6.0 Server Agent Unix/Win/Linux Upg/Comp Upg	40
Symantec Enterprise Security Manager 6.0 Server Agent WIN/UNIX/LNX/NTWR Gold Maint. 1YR	40

*Note: There is no separate charge for the Web server modules, just a charge for the 4 new Linux server agents since the application modules are now included in ESM 6.0.

Example #3

A year ago (in example #1), an organization purchased ESM and deployed it at its two main offices. ESM was installed on a total of 200 Windows NT/2000 servers, 100 UNIX servers, 10 Linux servers, 100 UNIX/Windows Workstations, 5 NetWare servers, 1 VMS server and 2 IBM iSeries (OS/390) platforms. The agents are controlled by two ESM managers (a UNIX manager with 3 CPUs at site A and a Windows 2000 Server Manager with a single CPU at site B). They would now like to renew their Gold maintenance for each license for an additional year.

Description	Qty
Symantec Enterprise Security Manager 6.0 Server Manager Gold Maint 1yr Rnw Value Band S	2
Symantec Enterprise Security Manager 6.0 Server Agent Unix/Win/Linux Gold Maint 1yr Rnw Value Band S	310
Symantec Enterprise Security Manager 6.0 Server Agent VMS/iSeries Gold Maint 1yr Rnw Value Band S	8
Symantec Enterprise Security Manager 6.0 Workstation Agent Gold Maint 1yr Rnw Value Band C	100
Symantec Enterprise Security Manager 6.0 Additional CPU Gold Maint 1yr Rnw Value Band S	2

Technical Support

The following maintenance and support options are available for purchase. Maintenance is a required purchase in the Symantec Security Licensing Program at the Elite level.



Telephone Support	Gold Maintenance	Platinum Support	Premium Platinum Support	Global Platinum Support ¹
Local Business Hours	●	●	●	●
Extended Hours (24 x 7 x 365)	○	●	●	●
Number of Support Incidents	Unlimited	Unlimited	Unlimited	Unlimited
Number Designated Callers	2	2	5	Custom
Additional Designated Caller(s)	Optional	Optional	Optional	Optional
Additional Language(s)	Optional	Optional	Optional	Optional
E-Services				
Standard Support Web Site	●	●	●	●
Platinum Web Site Password Protected	○	●	●	●
Security Alerting - Email, Phone, Pager, Fax, SMS	Optional	●	●	●
Technical Account Mgmt				
Technical Account Manager (TAM)	○	○	●	●
Global Technical Account Manager (GTAM)	○	○	○	●
Maintenance²				
Upgrade Insurance	●	●	○	○

¹Global Platinum is a custom option. Symantec account representatives assist customers in tailoring a global program to suit their needs.

²Platinum Maintenance is required to upgrade to higher tiers.

Target Market

Middle Market Segment

# of Nodes/Employees	Less than 500 users (Symantec defines middle market as
----------------------	--



	companies with minimum 100 to maximum 5000 employees).
Characteristics	<ul style="list-style-type: none">• Depend on a high degree of information confidentiality, integrity and availability for competitive survival• Possible industry or government regulation• Are involved in eBusiness or eCommerce initiatives• Have complex information systems consisting of large heterogeneous client/server networks, multiple geographic locations, supporting 500+ users.• Have multiple departments involved in providing information security, including an executive level manager, one or more dedicated information security managers, many functional network and systems managers, and perhaps internal auditors. (NOTE: These individuals may be ‘influencers’ or potential internal champions.)
Vendor Criteria	Trusted source
Product Criteria	<ul style="list-style-type: none">• Timely alerts on new vulnerabilities and malicious code.• Comprehensive vulnerability and malicious code information, covering all of the customer’s systems.• Alerts specific to each customer’s technologies.• Complete vulnerability and malicious code analysis, along with effective attack mitigation strategies and detailed patch information.
Influencers	IT Manager/Director Security Professional (including consultants)
Decision Maker	CxO (CIO, CFO, CEO) Senior executive (may work through or interface with IT or security officer; the smaller the company, the more likely the CxO is the decision maker)
Key Verticals	Include but are not limited to: <ul style="list-style-type: none">• Finance/banking• Communications• High tech• Government (especially military)• Application service providers• Internet service providers• Healthcare



Glossary

Policy Assessment: Checks performed against a system or applications to ensure the system or application is configured and being used in accordance with your corporate IT security policy.

Security Policy: A document that specifies what standards and controls are to be in place and followed in order to ensure availability, integrity and confidentiality of information assets. Many organizations will construct their internal security policies based in part on best practices as represented in industry standards like ISO 17799. In addition, many organizations will also adopt requirements as specified in industry specific regulations like HIPAA (Healthcare) or GLBA (Banking).

Vulnerability Assessment: Checks performed against a system or application to ensure that system or applications do not exhibit a known weakness that could be exploited, resulting in unauthorized use or misuse.

ESM Console: The user application that is used to control the ESM elements (i.e., managers and agents).

ESM Manager: The ESM component that 1) collects assessment data from ESM agents, 2) consolidates and stores the assessment data, and 3) stores configuration and operational information for the entire system.

ESM Agent: Platform (OS and/or Application) specific software that performs the assessment on the server or application. ESM agents install directly onto the systems that are being monitored.

Symantec, the Symantec logo and LiveUpdate are U.S. registered trademarks of Symantec Corporation. Enterprise Security Manager (ESM), Symantec Enterprise Security Architecture (SESA), Symantec Incident Manager, Symantec Security Management System and Symantec Security Response are trademarks of Symantec Corporation. All other brands and products are trademarks of their respective holder/s. Copyright © 2003 Symantec Corporation. All rights reserved.