

Symantec™ Critical System Protection

Proactive, behavior-based host intrusion protection that ensures host integrity and system compliance

Overview

Symantec™ Critical System Protection provides proactive behavior-based host intrusion protection through exploit prevention and system controls, along with monitoring, notification and auditing to ensure host integrity and compliance across heterogeneous platforms.

A centralized console enables administrators to configure, deploy, and monitor security policies; respond to alerts; and run reports on system activity across mixed platform environments.

Exploit prevention techniques shield the OS, applications, and services by defining acceptable behaviors and limiting false positives. System and device controls lock down configuration settings, file systems, and the use of removable media to protect systems from misuse by authorized people and programs. Integration with Symantec™ Security Information Manager allows customers to access additional event information to stay ahead of emerging threats. Communication of system and regulatory compliance status is easy and detail-rich with the graphical reports engine and its library of standard reports.

Key benefits

- Exploit prevention techniques shield operating systems, applications, and services by defining acceptable behaviors for each function
- Protects systems from misuse by authorized people and programs through system and device controls that lock down configuration settings, file systems, and the use of removable media
- Enterprise monitoring, notification, and auditing ensure host integrity, system and regulatory compliance
- Enterprise reporting capabilities enable cross-platform server auditing and compliance enforcement with graphical reporting engine that features multiple queries and graphic formats to visually highlight data
- Broad platform support – including Solaris, Windows, and Linux, with IDS functionality for AIX and HP-UX
- Centralized management console allows simplified, sophisticated administration of heterogeneous systems, reducing workload and providing better reporting
- Symantec Security Information Manager and SNMP integration enables additional event management information and incident correlation
- Libraries of best practice policies enable automated detection and localized reaction to known security events and vulnerabilities

What's New in release 5.1.2?

Platform Expansion

- Windows 2003 Standard & Enterprise x64 (EM64T, AMD64) Windows 2003 Standard & Enterprise R2
- Solaris 10 (SPARC32/SPARC64)
- Linux 2.6 kernels (x86, EM64T, AMD64)
- RHEL4
- SLES9
- HP Tru64 Unix version 5.1B-3 (IDS Only Support)
- HP-UX Itanium 2 (IA64)

Usability

- Event Wizard - A guided interactive dialog to automatically adjust policies or configurations to “deal with” selected events
- Improved policy authoring tools in console
- Multiple Real-Time Monitors (“NOCC like” display)
- Event viewing/reporting - easier navigation and viewing options

Policy Enhancements

- Unix C2 (security) Event Collector
- New IDS Rule types to process and take actions based on IPS events
- Numerous Authoring Tool improvements
- Extend stock Detection policy templates to include common customer use cases
- General improvements to Prevention and Detection Policies (ie Policy override support for UNIX/Linux)

Manageability and Integration

- Support for SQL Server 2005 Database
- Performance Improvements
- Event Purge Management
- User group modification
- Agent side event viewer
- Policy Override for Unix
- New detection capability for looking at file and property INI file changes

System requirements

Microsoft Windows - Agent

- Windows 2000 Professional / Server / Advanced Server
- Windows XP / Windows Server 2003
- Windows 2003 Standard & Enterprise x64 (EM64T, AMD64) Windows 2003 Standard & Enterprise R2
- 100 MB free disk space
- 256 MB of RAM

Microsoft® Windows NT - Agent

- Microsoft® Windows NT Server
- 100 MB free disk space
- 256 MB of RAM

SUSE Enterprise Linux 8/9 - Agent

- SUSE Enterprise Linux 8/9
- 100 MB free disk space
- 256 MB of RAM

System requirements - continued

Red Hat® Enterprise Linux ES 3.0/4.0 - Agent

- Red Hat® Enterprise Linux ES 3.0/4.0
- 100 MB free disk space
- 256 MB of RAM

Sun Solaris (Versions 8/9/10) - Agent

- Sun SPARC platform
- 100 MB free disk space
- 256 MB of RAM

IBM AIX 5L (Versions 5.1/5.2 and 5.3) - Agent

- POWER platform
- 100 MB free disk space
- 256 MB of RAM

HP-UX 11.23 (v2) - Agent

- Itanium 2 Platform (IA64)
- 100 MB free disk space
- 256 MB of RAM

HP-UX 11.i (Versions 11.11 and 11.23) - Agent

- PA-RISC platform
- 100 MB free disk space
- 256 MB of RAM

Symantec Critical System Protection 5.0 management server

- Microsoft Windows 2000 Server / Microsoft Windows Server 2003
- 1 GB disk space
- 1 GB of RAM
- Microsoft SQL Server

Symantec Critical System Protection 5.0 management console

- Microsoft Windows XP / Microsoft Windows 2000 Server / Microsoft Windows Server 2003
- 150 MB free disk space
- 256 MB of RAM

Datasheet: Intrusion Protection Symantec™ Critical System Protection

More information

Visit our web site

<http://enterprise.symantec.com>

To speak with a Product Specialist in the US

Call toll-free (800) 745-6054

To speak with a Product Specialist outside the US

Symantec has operations in 40 countries. For specific country offices and contact numbers, visit our web site.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

(408) 517-8000

(800) 721-3934

www.symantec.com

