Data Sheet: Intrusion Protection

Symantec™ Critical System Protection

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

Overview

Symantec Critical System Protection 5.2 offers protection for desktops and servers against malicious behaviors, blended threats, and known and unknown attacks by utilizing proactive, behavior-based Host Intrusion Protection through exploit prevention and system controls—along with Host Intrusion Detection based monitoring, notification, and auditing—with advanced log analysis and response capabilities to ensure host integrity and compliance across heterogeneous platforms. These capabilities provide effective countermeasures to protect servers from a security, compliance, and system configuration perspective. Exploit prevention techniques shield the OS, applications, and services by defining acceptable behaviors and limiting false positives, complementing reactive protection with proactive protection for comprehensive security. Critical System Protection also provides protection against internal abuse or mis-configuration, which is not detected or controlled by traditional security applications. This promotes both protection of critical assets and maintenance of regulatory compliance requirements. Finally, from a system configuration perspective, Critical System Protection system and device controls enable lock down configuration settings, file systems, and the use of removable media to protect systems from misuse by authorized people and programs or by unauthorized people using stolen credentials.

Symantec Critical System Protection has a centralized console that enables administrators to configure, deploy, and monitor security policies; respond to alerts; and run reports on system activity across mixed platform environments. It is integrated with Symantec LiveUpdate, Symantec™ Security Information Manager, and Symantec™ Managed Security Services to ensure timely updates of content as well as enterprise-level correlation and response capabilities.

Key benefits of Symantec Critical System Protection

Symantec Critical System Protection detects abnormal system activities, curtailing insider configuration changes that violate policies in addition to providing comprehensive prevention and detection capabilities to block viruses and worms and blunt hacking attacks and zero-day vulnerability attacks.

- Exploit prevention techniques shield operating systems, applications, and services by defining acceptable behaviors for each function
- Systems are protected 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 help ensure host integrity as well as system and regulatory compliance
- Enterprise reporting capabilities enable cross-platform server auditing and compliance enforcement with a 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®, and with Virtual Agent for unsupported and less common systems
- 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
- Flexible and customizable policies provide protection far greater than any other solution with little or no configuration, which minimizes setup time while maintaining a high degree of application compatibility

Features and technical specifications

What's new in release 5.2?

Usability

- Unified UNIX prevention and detection policies
- File differencing for Filewatch monitored ini/text files
- Console-based multiple custom prevention policies
- Simplified network protection setup (unified and firewall style)
- Finer-grained logging control
- Granular policy override and other override enhancements
- HTTPS/HTTP Agent installer option
- "Picklist" options for appropriate parameters

Advanced manageability and compatibility

- Virtual Agent for unsupported platforms
- ITA event collection—SCSP console shows SCSP and Intruder Alert (ITA) events
- Alerting via file output
- Command-line tool for queries
- Parameterized queries
- LiveUpdate performance improvement
- Trialware version

Security enhancements

- Memory injection protection
- Global Watch policy for correlation across different policies
- Module DLL control—policies based on DLLs calling a process
- IPS Service Event Collector

Platform expansion

- HP-UX 11i v3 (11.31) PA-RISC platform support

Symantec Critical System Protection 5.2 Agent system requirements

Microsoft® Windows

- Microsoft Windows® 2000

- Professional

- Server

- Advanced Server

- Microsoft Windows® XP

- Professional

- Home

- Microsoft Windows NT® Server
- Microsoft Windows Server 2003

- Windows 2003 Standard and Enterprise R2, including Service Pack 2 versions

- Windows 2003 Standard and Enterprise x64 (Intel® EM64T and AMD64)

- 100 MB free disk space
- 256 MB of RAM

Red Hat® Enterprise Linux ES (version 3, 4)

- x86 32-bit or x86 64-bit platforms (Intel EM64T and AMD64)
- 100 MB free disk space
- 256 MB of RAM

SUSE Linux Enterprise (version 8)

- x86 32-bit, AMD64, or IA-32 (Intel Itanium)
- 100 MB free disk space
- 256 MB of RAM

SUSE Linux Enterprise (version 9)

- x86 32-bit or x86 64-bit platforms (Intel EM64T and AMD64)
- 100 MB free disk space
- 256 MB of RAM

Solaris (version 8, 9)

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

Solaris (version 10)

- Sun SPARC platform or x86 64-bit platforms (Intel EM64T and AMD64)
- 100 MB free disk space
- 256 MB of RAM

IBM® AIX 5L (version 5.1, 5.2, and 5.3)

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

HP-UX 11.11 (11i v1)

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

HP-UX 11.23 and 11.31 (11i v2 and 11i v3)

- PA-RISC platform or Intel IA-64 platform (Itanium 2)
- 100 MB free disk space
- 256 MB of RAM

Symantec Critical System Protection 5.2 management server

- Microsoft Windows 2000 Server, Microsoft Windows Server 2003
- Minimum 1 GB free disk space; 40 GB or more recommended free space
- 1 GB of RAM
- X86 (Pentium® III 1.2 GHz or faster) or x86 64-bit (Intel EM64T or AMD64)

Symantec Critical System Protection 5.2 management console

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

More information

Visit our Web site

http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our Web site.

About Symantec

Symantec is a global leader in infrastructure software, enabling businesses and consumers to have confidence in a connected world. The company helps customers protect their infrastructure, information, and interactions by delivering software and services that address risks to security, availability, compliance, and performance. Headquartered in Cupertino, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
+1 (408) 517 8000
1 (800) 721 3934
www.symantec.com

Confidence in a connected world.