Data Sheet: Endpoint Security

Symantec™ Critical System Protection Monitoring Edition

Behavior-based host intrusion detection promoting host integrity and compliance

Overview

Symantec™ Critical System Protection Monitoring Edition detects changes and behaviors on virtual, physical and multi-OS systems to reduce operational downtimes and meet critical security and compliance requirements. The real time monitoring process oversees system, data and application files, registry keys, configuration settings and user and application behaviors on critical servers with minimal system impact. Monitoring Edition also supports meeting multiple regulatory and standards mandates like PCI-DSS Requirements 10.3, 10.5, 11.4 and 11.5. Flexible policy deployments across diverse infrastructures reduces administration overhead and unifies policy coverage. Instant detection and notification of threats as they occur reduces windows of exploit times and improves security efficacy.

Symantec Critical System Protection Monitoring Edition offers security and compliance monitoring for servers against malicious behaviors, file system changes and known and unknown attacks by utilizing Host Intrusion Detection based monitoring, notification, and auditing—with advanced log analysis capabilities to ensure host integrity and compliance across heterogeneous platforms. These capabilities provide effective system monitoring to protect servers from a security, compliance, and system configuration perspective. Critical System Protection Monitoring Edition provides notifications and alerts on internal abuses, privilege escalations and mis-configurations which are not detected by traditional security applications. From a system configuration perspective, Critical System Protection Monitoring Edition's system and device controls enable constant visibility into configuration settings, file systems, and the use of removable media to protect systems from misuse by authorized people and programs or by unauthorized users leveraging stolen credentials.

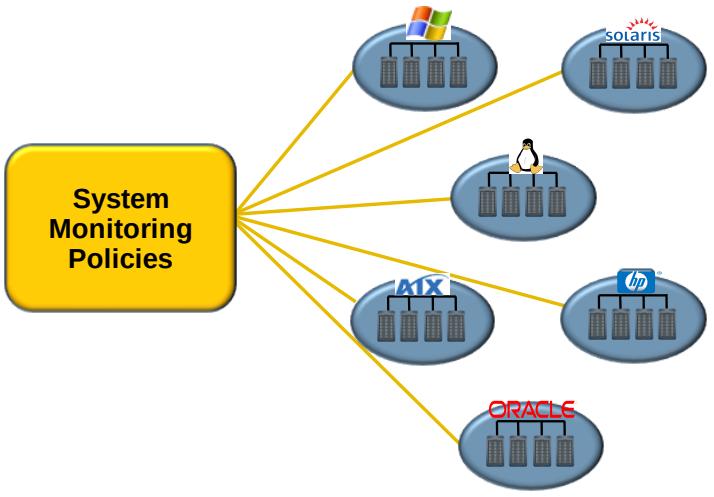
Symantec Critical System Protection Monitoring Edition has a centralized console that enables administrators to configure, deploy, and monitor security policies, respond to alerts and run reports on system activity across physical and virtual platform environments. It is also integrated with Symantec 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.

Symantec Critical System Protection Monitoring Edition is also fully upgradeable to Symantec Critical System Protection to enable advanced Host Intrusion Prevention capabilities with no reinstallation required.

Key Features and Benefits

Symantec Critical System Protection Monitoring Edition detects unwanted or abnormal system activities, insider configuration changes that violate policies and provides comprehensive detection for virus and worm behaviors as well as blunt hacking and zero-day vulnerability attacks.

- **Real time monitoring** – Increases detection of changes to system, data and application files, registry keys, configuration settings and notifies on inappropriate user and application behaviors.
- **Policy and behavior based operation** – Improves protection posture without compromising system performance.
- **Virtual hosts and guest monitoring** – Monitors the virtual host (console OS/hypervisor) and guest VMs for intrusions, mis-configurations and inappropriate accesses for better security and compliance.
- **Policy groupings based on asset profiles** – Enables quick and flexible deployment of uniform policies across diverse infrastructure requirements.
- **Out-of-the-box compliance templates** – Automates policy creation and Improves reporting with pre-defined templates for common mandates such as PCI.
- **Custom policy creation** – Reduces complexity with easy rule administration and minimized rules sets.
- **Real time threat assessment** – Lowers risk through instant detection and notification of threats as they are occurring to reduce windows of exploit times.
- **Event logging and reporting** – Promotes effective host integrity and efficient demonstration of compliance with consolidated event logs and advanced log analysis capabilities for high availability and security across heterogeneous platforms.
- **Integration with SIEM** – Data collectors are built for Symantec SIM and third-parties to enable real-time log management and correlation.



Data Sheet: Endpoint Security

Symantec™ Critical System Protection Monitoring Edition

Behavior-based host intrusion detection promoting host integrity and compliance

	OS Platform Support	System Requirements
Symantec Critical System Protection Management Server	Microsoft®Windows® 2000 Server / Microsoft® Windows® Server 2003 / Microsoft® Windows® Server 2008, 32-bit and 64-bit, including SP2 and R2 SQL Enteprise Server 2005 SP2, SQL Enterprise Server 2005 Express, SQL Enterprise Server 2008, 32-bit and 64-bit	1 GB of disk space 1 GB of RAM
Symantec Critical System Protection Management Console	Windows 2000 Server / Windows Server 2003 / Microsoft® Windows® XP, 32-bit and 64-bit Java client or Web Console	150 MB of disk space 256 MB of RAM
Microsoft Windows - Agent	Microsoft® Windows® 2000 Professional / Server / Advanced Server / / Windows Server 2003, 32-bit and 64-bit, including R2 and SP2 versions / Windows Server 2008, 32-bit and 64-bit, including R2 and SP2 versions, Microsoft® Windows® NT Server, x86 32-bit, Intel EM64T or AMD 64 platforms	100 MB of disk space 256 MB of RAM
Microsoft Windows NT - Agent	Microsoft® Windows® NT Server	
SUSE Enterprise Linux (8, 9, and 10) Agent	x86 32-bit, Intel EM64T or AMD 64 platforms	
Red Hat Enterprise Linux ES (3.0 , 4.0, and 5.0)	x86 32-bit, Intel EM64T or AMD 64, Hugemem (32-bit) platforms	
Sun Solaris (8, 9 and 10) Agent	Sun™ SPARC; SPARC32/SPARC64; EM64T or AMD64 platform (V10 only)	
VMWare ESX 3.5 Console OS	x86 32 bit	
IBM AIX 5L (5.1, 5.2, 5.3 and 6.1) Agent (IDS Only)	POWER PC platform 32-bit and 64-bit	
HP-UX 11.23 and 11.31 (11i v2 and v3) Agent	PA-RISC or Itanium 2 platform (IA64) 64-bit	
HP-UX 11.i (11.11) Agent	PA-RISC platform 64-bit	
HP Tru64 Unix 5.1B-3 Agent	Alpha platform	

Visit our website
http://enterprise.symantec.com

To speak with a Product Specialist in the U.S.
Call toll-free 1 (800) 745 6054

About Symantec
Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec World Headquarters
350 Ellis Street.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com