Symantec™ Host IDS

Intrusion detection and prevention technology with advanced management capabilities

Because organizations rely on the Internet for communication, collaboration, and commerce, they need security solutions that keep intruders out, while providing secure access to customers, partners, and remote employees. Firewalls and strong authentication processes help to secure systems from unauthorized access, but they do little to protect against hackers or authorized users with malicious intent. Symantec Host IDS complements firewalls and other access controls by delivering host-based intrusion protection with advanced management capabilities to detect signs of system misuse and prevent security problems. The combination of prevention and detection technologies within the product facilitates the critical balance between server security and server performance.

> Process Management technologies

Process Management capabilities combine multiple intrusion prevention technology functions—including process monitoring, blocking, and reporting. By allowing administrators to view more granular process information, set flexible server security monitoring options, and define policies to block unauthorized server processes before they start, organizations can respond rapidly to intrusions, make informed server security policy decisions to protect critical servers.

- Process Monitor allows administrators to define a wide variety of security configurations to provide a fault-tolerant, secure environment tailored to the organization’s security policy
- Process Blocker restricts server abilities and protects against malicious processes through defined configurations
- Process Reporter provides access to granular process data so administrators can make rapid, informed decisions regarding server security

> Real-time detection and response

Symantec Host IDS provides real-time monitoring, detection, and prevention of security breaches, delivering automated policy enforcement and incident response for servers, applications, and data. As an additional line of defense behind the firewall, it enables administrators to develop proactive policies to stop hackers or authorized users with malicious intent from misusing systems. If systems are threatened, Symantec Host IDS will notify administrators with an alarm and take precautionary action, in order to prevent the loss or theft of information.

> Centralized management

With predefined security rules and security reports, administrators can gain control over systems with policy-based monitoring that determines which systems and activities to monitor and what actions to take if intrusions or misuse occurs. Through a centralized management console, administrators can create monitoring and response policies, apply new rules, centrally collect and archive audit logs for incident analysis and graphical reporting, and automatically receive the latest intrusion detection signatures via LiveUpdate. The management console also allows administrators to define a hierarchy of security roles without compromising security. A new,

KEY POINTS

- Monitors systems in real time to detect and respond to security breaches and other unauthorized activities
- New! Process Management capabilities combine multiple intrusion prevention technology functions to allow organizations to respond rapidly to intrusions and make informed server security policy decisions to protect critical servers
- Enables the creation of customizable host-based intrusion protection policies and responses
- Centralized management tools simplify the monitoring and enforcement of host intrusion protection security policies
- Integrates with the Symantec™ Security Management System to deliver enhanced prioritization, identification, containment, and removal of security threats
- Provides audit data for incident and forensic analysis and generates graphical reports of intrusion activity
- New! Intuitive, Java™-based Policy Editor simplifies the development and deployment of policies for the Symantec Host IDS sensors/agents
- Protects information assets with a complete library of intrusion detection signatures and updates delivered from Symantec™ Security Response

Intrusion Protection

SECURITY TECHNOLOGY

Symantec™ Host IDS

Intrusion detection and prevention technology with advanced management capabilities
intuitive, Java™-based policy editor develops and deploys policies to thousands of sensors/agents in a few steps. Specialized software agents are included that support server platforms running Windows® 2000, Windows NT® 4.0, Windows XP, Sun™ Solaris™ 8 and 9, AIX 5.1/5.2, HP-UX 11i, RedHat Linux 7.3 and Windows 2003, and can be configured to monitor Web or database applications running on Windows NT and Windows 2000 platforms.

Symantec™ Security Management System integration

Symantec Host IDS integrates with the Symantec Security Management System, a management framework that provides consolidated data collection, logging, and reporting for Symantec and select third-party products. With the Symantec Security Management System, administrators are able to identify and prioritize security threats, view security alerts, and manage incident containment and response for a range of security products across the entire enterprise.

Backed by Symantec™ Security Response

Symantec Security Response offers a range of powerful security resources, including world-class product support, and the nonstop 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.

Symantec has worldwide operations in 36 countries. For specific country offices and contact numbers please visit our Web site.

SYSTEM REQUIREMENTS

Symantec Host IDS utilizes the Symantec™ Enterprise Security Architecture (SESA) to provide integration and management across a wide range of leading security products. Symantec Host IDS includes the SESA Foundation pack, a set of scalable, extensible, and secure technologies that make Symantec Enterprise Security products interoperable and manageable.

Installation of the SESA Foundation is required prior to installing this product agent machine.

CONSOLE MACHINE

• Microsoft® Internet Explorer 5.5 or higher

WORLD HEADQUARTERS

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

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

Copyright © 2003 Symantec Corporation. All rights reserved. Printed in the U.S.A. 11/03  All product information is subject to change without notice.