



Symantec ManHunt™

High-speed, advanced network intrusion protection

Businesses and consumers alike increasingly rely on the Internet to conduct high value transactions. Publicly accessible networks can be the target of theft, vandalism, and snooping as attacks against corporate and federal networks have grown in number, sophistication, and in terms of malicious intent. Certain attacks, such as denial-of-service (DoS) attacks, interrupt normal business operations by flooding a site with unwanted traffic, rendering the site inaccessible. These attacks are easily generated and can wreak havoc on the most sophisticated networks. In addition, blended threats such as the Code Red and Nimda worms can penetrate firewalls and result in costly damages and extensive clean-up time.

To address these growing concerns, corporations often deploy security products such as firewalls and intrusion detection and prevention technologies to provide some defense. But when using these products, enterprises must invest significant time and resources to gather the security intelligence that can help them protect networked assets. Symantec ManHunt provides advanced, high-speed network intrusion detection, correlation and analysis, and proactive prevention and response to protect corporate networks against costly intrusions and denial-of-service (DoS) attacks.

> Ultra high-speed intrusion detection

Symantec ManHunt sets a new standard in network intrusion protection with high-speed traffic monitoring, allowing implementation at virtually any level within an organization, even on gigabit backbones. By implementing customized drivers for high-traffic enterprise networks, Symantec ManHunt provides high-speed network intrusion detection—at speeds of up to 2 gigabits per second—without dropping packets.*

> Hybrid threat architecture enhances protection

As attacks become more sophisticated and less intrusive, traditional intrusion detection products lack the capability to discern coordinated, stealthy tactics. Symantec ManHunt's hybrid detection architecture uses an array of methodologies to effectively and accurately detect sophisticated attacks as they emerge. These advanced techniques enable Symantec ManHunt to identify known and unknown or zero-day attacks, while decreasing false positives.

By analyzing network traffic using protocol anomaly detection, rather than solely relying on prior signatures, Symantec ManHunt identifies new and unknown attacks even before signatures are published. This capability, called zero-day detection, eliminates the window of vulnerability present in traditional signature-based intrusion detection products to ensure the network is not left exposed. Additionally, the traffic rate monitoring capability allows for detection and protection against stealth scans and denial-of-service attacks that can cripple even the most sophisticated networks.

KEY POINTS

- > Protects enterprise networks with multi-gigabit detection at speeds up to 2 gigabits per second
- > Identifies known and unknown or "zero-day" attacks and protects against denial-of-service attacks and stealth scans
- > Analysis engine dramatically reduces the effort required by security personnel to identify threats
- > Scalable and flexible deployment options help reduce total cost of ownership
- > **NEW!** Rapid and scheduled security updates provide top-tier protection
- > **NEW!** Red Hat® Linux® operating system support
- > **NEW!** Role-based administration options enable hierarchical levels of user access
- > Backed by Symantec™ Security Response, the world's leading Internet security research and support organization

* Note: Multi-gigabit speeds are dependent on system configuration.

> **Analysis and correlation**

INTEGRATED, REAL-TIME EVENT CORRELATION AND ANALYSIS

A state-of-the-art correlation and analysis engine filters out erroneous data and refines only the relevant information, providing threat awareness without data overload. Symantec ManHunt's real-time analysis engine gathers intelligence across the network using cross-node correlation to spot trends and recognize events occurring within the dispersed network in real-time. This correlation and analysis capability reduces the effort required to identify threats, allowing security personnel to focus on more sophisticated intrusion investigation and policy management, instead of wasting hours examining uncorrelated event logs.

PROACTIVE PREVENTION AND RESPONSE

Symantec ManHunt surpasses passive incident identification and alerting to actively defend an organization's network assets. With proactive prevention and response technologies, this network intrusion protection solution contains and controls attacks in real-time and initiates other actions required for incident response. Symantec ManHunt prevents attacks by terminating TCP sessions and supporting the implementation of custom responses. It also sends email and SNMP notifications to aid in the response process and protect an enterprise's most critical assets.

FULL PACKET CAPTURE AND INTEGRATED PACKET FILTERING

A complete log of an offending packet aids in effective analysis and identification of attack characteristics. Symantec ManHunt can be configured on a per-interface basis to capture the entire packet of a suspected event. Traffic parameters including source and destination port and IP address, protocol type, packet size, and time period help administrators quickly determine whether the packet is a benign event that can be filtered or a malicious event that should be flagged for further investigation. If the incident requires further analysis, Symantec ManHunt provides the ability to query current and previously exports flows. Additionally, integrated logging and analysis enables administrators to drill down to captured packets and keystrokes for specific forensic details. This unique analysis capability enables security specialists to capture everything from the full pipe stream down to a few packets in the same connection.

> **Management and Deployment**

LOWER TOTAL COST OF OWNERSHIP

Symantec ManHunt provides scalable and flexible deployment options that help reduce the total cost of ownership for an enterprise. The scalable architecture enables a single node to monitor multiple segments, switch ports, or VLANs. As the network infrastructure grows, network interface cards can be added to the same node to support additional monitoring requirements. By deploying fewer machines, administrators reduce the overhead required to manage and maintain a network intrusion protection solution.

To further strengthen network defenses in mission-critical environments, multiple Symantec ManHunt nodes can be deployed in a High Availability (H/A) configuration to ensure uptime and uninterrupted protection. Each Symantec ManHunt device intelligently distributes traffic flow between processing units for internal load balancing. Should the primary node in the H/A group fail, the secondary node will seamlessly take over without any loss of traffic or flow data.

CENTRALIZED CLUSTER MANAGEMENT

A Symantec ManHunt deployment may consist of sensor nodes arranged in large clusters, all managed through a single administration console. Every communication between Symantec ManHunt nodes and the management console is authenticated and AES-256 encrypted to ensure that Symantec ManHunt node cluster management and monitoring is secure, even at remote office locations. Improved capabilities from the Symantec ManHunt console include cluster-wide management of security updates, licenses, users, and signatures.

ROLE-BASED ADMINISTRATION

Symantec ManHunt provides the ability to define administrative users and designate roles that grant users varying levels of access rights. Administrative users can be assigned roles ranging from full privileges to restricted user access that only allows event monitoring without packet inspection capabilities. All administrative changes made from the console are logged for auditing purposes.

ENHANCED REPORTING

Symantec ManHunt includes multiple levels of reporting, offering data drill-down and threat status summaries to help quickly spot associated events and attack trends. Reports can be generated in text, HTML and PDF formats and can be emailed, saved, or printed. New reporting enhancements include support for scheduled and HTML-formatted console reports, and the ability to print reports from the console. In addition, scheduled reports can also be archived to a remote machine using secure copy. With its reporting features, Symantec ManHunt enables organizations to measure the overall effectiveness of the security infrastructure, meet operational objectives for measuring security effectiveness, disseminate security information, and track compliance across the organization.

> **Backed by Symantec™ Security Response**

Symantec Security Response, the world's leading Internet security response team, works around the clock to research security threats and provide rapid and scheduled security updates that help maintain up-to-date attack and vulnerability protection. The security updates include signatures, and exploit and vulnerability information. Symantec's response organization also responds rapidly to attack outbreaks to help protect against ever-increasing, real-time threats.

For more information about Symantec ManHunt, visit
<http://www.enterprisesecurity.symantec.com>

INTRUSION PROTECTION IS A KEY COMPONENT OF SYMANTEC ENTERPRISE SECURITY. SYMANTEC ENTERPRISE SECURITY COMBINES WORLD-CLASS TECHNOLOGIES, COMPREHENSIVE SERVICES, AND GLOBAL EMERGENCY RESPONSE TEAMS TO HELP BUSINESSES RUN SECURELY AND WITH CONFIDENCE.

SYSTEM REQUIREMENTS
SYMANTEC MANHUNT 3.0

OPERATING SYSTEM REQUIREMENTS

Solaris

- Sun® 64-bit Solaris™ 8
- Sun® Solaris 8 Intel® Platform Edition
- Java™ 2 Runtime Environment, standard edition 1.2.2

Linux

- Red Hat Linux 8.0 with kernel 2.4 (on Intel processors)
- Java™ 2 Runtime Environment, standard edition 1.4

MEMORY REQUIREMENTS

- 512MB-1GB RAM for Fast Ethernet configurations
- 2GB RAM for single-Gigabit configurations
- 4GB RAM for multi-Gigabit configurations

HARDWARE REQUIREMENTS

- Symantec ManHunt-certified platform and hardware configuration
- 1 Network Interface for each monitored device (up to 12 fast Ethernet or 6 gigabit Ethernet)
- 1 Network Interface for administration/management

SYMANTEC MANHUNT CONSOLE REQUIREMENTS

- Java™ 2 Runtime Environment v1.4
- Microsoft® Windows® 2000/XP, Red Hat Linux 8.0, Solaris 8
- 256 MB RAM

WORLD HEADQUARTERS

20330 Stevens Creek Blvd.
Cupertino, CA 95014 USA
408.517.8000
800.721.3934

www.symantec.com

For Product information
in the U.S. call toll-free
800.745.6054

Symantec has worldwide
operations in 38 countries.
For specific country
offices and contact numbers
please visit our Web site.

