Dragon™ Host Sensor

- Host-based intrusion defense via a modular, flexible architecture for today's most common operating system
- Protects at the host and application level by monitoring the operating system and crucial applications
- Application Intrusion Prevention module averts attacks on the most commonly targeted applications—DNS servers, mail servers, web servers

- **Application Intrusion Prevention**
  - Averts attacks on the most widely used web applications, IIS and Apache
- **File attribute monitoring**
  - Monitors file attributes such as owner, group, permissions, file size
- **File integrity checking**
  - Monitors files or directories to determine if content has been changed via MD5 hash
- **Log file analysis**
  - Analyzes any file or directory against a signature policy
- **Windows event log analysis**
  - Monitors Windows event logs for sign of misuse or attack
- **Windows registry analysis**
  - Analyzes the Windows registry for attributes that should not be accessed and/or modified
- **TCP/UDP service detection**
  - Monitors for opened TCP and UDP ports, providing critical protection against backdoor services
- **Kernel monitoring**
  - Detects suspicious privilege escalations and other signs of kernel-level compromise
- **Custom module interface**
  - Provides an open and easy interface for custom module development

Scalable, Flexible Host-Based Intrusion Defense

A host-based intrusion defense tool, Dragon Host Sensor prevents web attacks and monitors individual systems running today's most common operating systems, for evidence of malicious or suspicious activity in real time.

Dragon Host Sensor may be deployed on a protected host where it uses a variety of techniques to detect attacks and misuse on the system, including analyzing the security event log, checking the integrity of critical configuration files, or checking for kernel-level compromises. This hybrid approach ensures that no misuse goes undetected.

Dragon Host Sensor may also be deployed on a dedicated analysis system where logs are forwarded and analyzed from most commercial firewalls, routers, switches and other IDS devices. Correlating events from these devices and from Dragon Network and Host Sensors is critical in identifying which events are the most serious, as well as understanding their origin and impact.

The new Dragon Host Sensor**Application Intrusion Prevention** module averts attacks on the most commonly targeted applications—such as DNS servers, mail servers, and web servers running Microsoft IIS and Apache.

Using non-conventional techniques to identify attempted intrusions or general misuse, the Host Sensor can be installed on a dedicated system to create a "deceptive" server designed to entice an alarm on attempted intrusions by simulating a fake web server, telnet server, or mail server.

Dragon Host Sensor deploys advanced techniques in identifying root-kits and buffer overflows via its kernel-monitoring module. This module traps and analyzes all calls into the kernel and can identify the existence of any kernel-level root-kit, an absolute requirement in identifying compromised systems before an attacker completely covers their tracks. It can also identify anomalous privilege escalations states resulting from successful buffer overflows. Dragon's kernel monitoring capabilities are an essential building block on the path to host-based intrusion prevention—failure to implement this step leaves the host open to attacks that other intrusion prevention solutions cannot detect.

Centrally managed via **Dragon Enterprise Management** Server for signature and configuration updates, Dragon Host Sensor also reports all information—including event description, source/destination IP, source/destination port, raw log (if applicable) and timestamp—to the Security Information Management functionality within Dragon Management Server for real-time alerting, forensic and trend analysis.

enterasys™
Networks that Know

Specifications

Technical Specifications

Operating Systems

Dragon Host Sensor: Windows NT/2K/XP, Sparc Solaris (versions 8 and 9), AIX (versions 4.3.3 and 5.X), HPUX (version 11.x), and Linux Distributions: Red Hat (versions 8.0 and 9.0), SuSE (version 8.1), Mandrake (version 9), Slackware (version 8.1) and Debian

Ordering Information

Host Sensor Software

DSHSS-WIN
Dragon Host Sensor software for Windows

DSHSS-LNX
Dragon Host Sensor software for Linux

DSHSS-SOL
Dragon Host Sensor software for Solaris

DSHSS-HPX
Dragon Host Sensor software for HP-UX

DSHSS-AIX
Dragon Host Sensor software for AIX

Warranty

As a customer-centric company, Enterasys is committed to providing the best possible workmanship and design in our product set. The Dragon product family includes a ninety (90) day warranty for software that covers defects in media only, and a one (1) year warranty for hardware.

Service and Support

Enterasys understands that superior service and support is a critical component of *Networks that Know*.™ The Enterasys **SupportNet Portfolio**—a suite of innovative and flexible service and support offerings—completes the Enterasys solution. SupportNet offers all the post-implementation support services you need—online, onsite or over the phone—to maintain your network availability and performance.

Additional Information

For more information about Enterasys Dragon, visit the web at **http://www.enterasys.com/products/ids**

Contact Information

Contact Enterasys Sales at **877-801-7082** or enterasys.com/

Enterasys Networks
Corporate Headquarters
50 Minuteman Road
Andover, MA 01810
U.S.A

Dragon is a registered trademark of Enterasys Networks. All other products or services mentioned are identified by the trademarks or service marks of their respective companies or organizations. NOTE: Enterasys Networks reserves the right to change specifications without notice. Please contact your representative to confirm current specifications.

Lit. #9013546 3/04

enterasys™
Networks that Know