Security and Intrusion Defense for Enterprise Networks

Designed specifically to meet the unique security requirements of the enterprise environment, the Dragon 6.1 Intrusion Defense System offers comprehensive features that minimize network vulnerabilities and bring improved security to the enterprise. Only Dragon, with its unique network-based detection and response capabilities, modular host intrusion detection components, server management, and event management provides a reliable solution for detecting and responding to the broad array of attacks present in today’s constantly changing security landscape.

The Dragon 6.1 Intrusion Defense solution includes:

- **Dragon Host Sensor**—Host-based intrusion defense, delivered via a modular and flexible architecture for today’s most common operating systems, protects at the host and application level by monitoring the operating system and critical applications via a variety of techniques.
- **Dragon Enterprise Management Server**—Tools and technology for highly scalable management and decision support across the enterprise.
  - **Policy Management**—Centralized command and control of network and host sensors with system-level deployment of configuration and protection policies
  - **Security Information Management**—Centralized security alert information and web-based analysis tools for real-time event monitoring, advanced analysis and reporting
  - **Event Flow Processors**—Collect and aggregate events to create a hierarchical event management system for local monitoring of events and aggregated enterprise-wide events monitoring correlation

- **Complete intrusion defense**
  - Integrated network- and host-based intrusion defense, and scalable enterprise management
  - Flexible software and hardware-based solution with support for Windows, Linux, Solaris, AIX and HP-UX hosts
- **Stops hackers in their tracks**
  - Variety of Active Response features that include terminating sessions and reconfiguring firewalls, switches and routers
- **Highly scalable architecture**
  - Scalability, availability and redundancy for all enterprises
- **Enterprise-wide security monitoring**
  - Monitors third-party routers, switches, firewalls, applications, web servers and other intrusion detection products
- **Extensive statistics and information gathering**
  - High visibility with real-time reporting and historical forensics
  - Executive-level reporting
- **Leading detection capabilities**
  - Multimethod detection including pattern matching, protocol decoding, and anomaly detection
  - Largest signature base in breadth, depth and quality; signatures updated continuously

• A complete intrusion defense system with scalability to meet the requirements of enterprises of all sizes and types
• Powerful and responsive enough to stop hackers in their tracks
• Leading multimethod detection capabilities with the largest signature base in breadth, depth and quality for monitoring across the entire infrastructure
Dragon Network Sensor—Powerful Network Intrusion Defense

A sophisticated software and appliance-based network intrusion defense system, the Dragon Network Sensor identifies misuse and attacks across the network.

Placed at network aggregation points, the Dragon Network Sensor is unmatched in detecting intrusions via signature, protocol, and anomaly-based techniques. Application-based event detection detects non-signature-based attacks against commonly targeted applications including HTTP, RPC and FTP. These multimethod detection techniques, combined with an extensive, frequently updated signature database and false-positive tuning capabilities, ensure that no intrusion goes undetected.

When an attack is detected, Dragon Network Sensor employs a variety of Active Response techniques to block the would-be intruder, including taking action to stop the sessions and reconfiguring firewall policies or switch and router Access Control Lists.

Dragon Network Sensor offers market-leading deep Forensics capabilities, including flexible packet capture, complete session reconstruction, and highly configurable Session VCR (collects all session information for services such as HTTP, FTP, POP and certain IPs or networks) that is needed to analyze network-based attacks.

Dragon Network Sensor is centrally managed via Dragon Enterprise Management Server, which provides signature and configuration updates, as well as reporting and event management, including event description, source/destination IP, source/destination port, offending packet, session (if configured), and timestamp.

Features Include:

- **Open tunable signatures** allow implementation, modification, and custom creation of a set of signatures designed to detect the attacks that apply to each unique environment

- **Multi-interface monitoring** combines multiple network interfaces into a single traffic stream for analysis, enabling a dual-tap solution—without a switch

- **IP defragmentation and TCP/UDP stream reassembly** identifies attackers who attempt to evade an IDS by distributing attacks over multiple packets

- **Protocol decoding** identifies attackers who attempt to hide an attack within an application protocol for most commonly targeted protocols

- **IDS Denial of Service (DOS) countermeasures** defeats tools such as “stick” and “snot” that attempt to DOS an intrusion detection system

- **Event sniping** terminates an attack session via a TCP reset or ICMP unreachable message, stopping the attack before real damage can occur

- **Dynamic reconfiguration** stops attacks through Checkpoint firewalls and with custom scripts can block hackers on most commercial switches and routers

- **Probe prevention** defeats or confuses many scanning techniques by issuing false responses to the probe, misleading attackers about the true nature of the network and/or target system

- **Backdoor and rogue server detection** detects backdoors and rogue servers using varied techniques
Dragon Host Sensor—Scalable, Flexible Host-Based Intrusion Defense

A host-based intrusion defense tool, Dragon Host Sensor monitors individual systems and applications, including today’s most common operating systems, for evidence of malicious or suspicious activity in real time, and monitors key system logs for evidence of tampering.

Dragon Host Sensor may be deployed on a protected host (on-host) or on a dedicated analysis system where logs are forwarded and aggregated via SNMP or syslog from routers, switches and other IDSs.

Dragon Host Sensor uses a variety of techniques to detect attacks and misuse on a protected 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 is able to monitor and analyze the output 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. In addition, Dragon Host Sensor monitors the most commonly attacked applications—such as DNS servers, mail servers, and web servers, including Microsoft IIS and Apache. Dragon Host Sensor can also monitor a local system for new services, which is essential in identifying backdoors or unauthorized applications that may have been installed via an “out-of-band” attack or worm.

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.

In addition, 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—both known and new, an absolute requirement in identifying compromised systems before an attacker is able to completely cover 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.

Features Include:

- **File attribute monitoring** monitors specific file attributes such as owner, group, permissions and file size
- **File integrity checking (MD5)** monitors files to determine if content has been changed via MD5, to ensure that sensitive files, which should not be modified, have not been modified
- **Log file analysis** analyzes any file—including the system log, security log, or the log of a custom-built application—against a signature policy
- **Windows event log analysis** monitors the various 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, essential in identifying attacks against often-targeted Microsoft servers
- **TCP/UDP (backdoor) service detection** monitors for opened TCP and UDP ports, providing critical protection against backdoor services, which can be used to allow unauthorized access through the firewall or act as a staging point for a distributed denial of service or outright attack
- **Kernel monitoring** detects suspicious privilege escalations and other signs that the kernel has been compromised
- **Custom module interface** provides an open and easy interface for custom module development, allowing the customers to write their own modules for Dragon Host Sensor
Dragon Enterprise Management Server—Complete Monitoring and Control

**Dragon Enterprise Management Server** is made up of a number of highly integrated technologies. Web based and centralized, **Policy Management** tools offer enterprise-wide management of small and large-scale Dragon deployments. Dragon Policy Manager provides centralized management of the Dragon Network and Host Sensors, while Alarntool offers centralized alarm and notification management.

A centralized collection of all security alert information, **Security Information Management** applications provide monitoring, analysis, and reporting of security events across the enterprise.

Finally, **Event Flow Processors** collect and analyze logs from firewalls, routers, switches, applications and even third-party intrusion detection systems for log aggregation, analysis and event forwarding, providing for highly scalable and flexible architectures.

**Additional Dragon 6.0 Appliances**

Dragon’s **Integrated Network Sensor/Server** is an all-in-one solution for remote/branch offices that require a single system for network-based intrusion detection, log aggregation, and local management/monitoring. The Integrated Network Sensor/Server includes the Dragon Network Sensor for network monitoring; Dragon Host Sensor for local protection, log aggregation and analysis; and Enterprise Management for local management, monitoring, and event processing.

**Features Include:**

- **Web-based management** interface allows platform-independent administration of the IDS system from any browser
- **Software authentication** for different user types
- **Continuous signature updates** ensure customers are covered, even from the most recent attacks; available live via SSL
- **System-level management** enables all network or host sensors to be configured and updated simultaneously with new configuration parameters or signatures
- **Custom signature development** allows customers to create their own signatures to detect whatever events are most critical to each environment
- **Event analyzer** allows the customer to view events in either real time or from a historical perspective, to maintain a clear understanding of the state of the security system
- **Management reports** offer easy-to-understand aggregated data on the events detected, and the timeframe of detection
- **Real-time monitoring** allows events to be viewed as they occur, providing an understanding of what may have changed, or what is happening at that moment within the security system
- **Session reconstruction** allows the user to view the entire session related to an event, including the packets involved
**SPECIFICATIONS**

**TECHNICAL SPECIFICATIONS**

**FE50 Dragon Network Sensor Appliance**
- Performance rating: 50 Mbps
- Architecture: Intel PIII
- Memory: 256 MB, 20 GB IDE hard drive
- NICs: 3 10/100 copper
- Supports multi-interface monitoring

**FE200 Dragon Network Sensor Appliance**
- Performance rating: 200 Mbps
- Architecture: Dual Intel PIII
- Memory: 512 MB, 18 GB SCSI hard drive
- NICs: 2 10/100 copper, 1 10/100/1000 copper
- Supports multi-interface monitoring

**GE200 Dragon Network Sensor Appliance**
- Performance rating: 200 Mbps
- Architecture: Dual Intel PIII
- Memory: 512 MB, 18 GB SCSI hard drive
- NICs: 2 10/100 copper, 1 Gigabit fiber
- Supports multi-interface monitoring

**GE500 Dragon Network Sensor Appliance**
- Performance rating: 500 Mbps
- Architecture: Dual Intel XEON
- Memory: 1024 MB, 18 GB SCSI hard drive
- NICs: 2 10/100/1000 copper, 2 Gigabit fiber or copper Gigabit
- Supports multi-interface monitoring

**Dragon EFP Appliance**
- Architecture: Dual Intel PIII
- Memory: 512 MB, 72 GB SCSI hard drive
- NICs: 2 10/100 copper

**Dragon Enterprise Management Server Appliance**
- Architecture: Dual Intel PIII
- Memory: 1024 MB, 72 GB SCSI hard drive
- NICs: 2 10/100 copper

**Integrated Network Sensor/Server**
- Architecture: Dual Intel PIII
- Memory: 1024 MB, 36 GB SCSI hard drive
- NICs: 2 10/100 copper, 1 10/100/1000 copper or 1 Gigabit fiber
- Supports multi-interface monitoring

**Operating Systems**
- Dragon Network Sensor: Sparc Solaris (versions 8 and 9), Red Hat Linux (2.4 kernel, versions 7.3 and 8.0)
- 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 7.3 and 8.0), SuSE (version 8.1), Mandrake (version 9), Slackware (version 8.1) and Debian
- Dragon Enterprise Management: Sparc Solaris (versions 8 and 9), Red Hat Linux (versions 7.2 and 7.3)

**PHYSICAL SPECIFICATIONS**

**Form Factor**
- 1U rack-mount server chassis for EIA standard 310-D racks

**Dimensions**
- 4.32 cm (1.7") H X 48 cm (18.9") W X 61.21 cm (24.1") D
- 4.32 cm (1.7") H X 42.9 cm (16.9") W X 60.71 cm (23.9") D (GE500 only)

**Front Panel (Buttons)**
- Power on/off button (momentary), system-reset button, ACPI sleep switch system ID button, and tool-activated NMI switch

**Front Panel (LEDs)**
- Power, hard drive activity, network activity, system ID, and general system fault

**ENVIRONMENTAL SPECIFICATIONS**

**Operating Temperature**
- +10º C to +35º C (50º F to 95º F)
- +5º C to +35º C (41º F to 95º F) (maximum change not to exceed +10º C) (GE500 only)

**Non-Operating Temperature**
- -40º C to +70º C (-40º F to 158º F) (ambient)

**Non-Operating Humidity**
- 95% at 30º C (non-condensing)

**Power Consumption**
- Voltage Range: 4.8 Amp at 115V
- Voltage Range: 2.9 Amp at 220V

**GE500 Only**
- Voltage Range: 4.96 Amp at 115V
- Voltage Range: 2.48 Amp at 220V
AGENCY AND STANDARDS SPECIFICATIONS

Safety
Europe/CE Mark: EN60950 (complies with 73/23/EEC)
International: IEC60950 (CB Report and Certificate)
Korea: K-Mark
Nordic Countries: NEMKO/EMKO–TSE (74-SEC) 207/94
Russia: GOST 50377-92
U.S., Canada: UL1950 – CSA 950 (UL and cUL)

GE500 Only
Argentina: IRAM Certificate
Australia/New Zealand: AS/NZS 3260 (covered by CB report)
Belarus: Bellis Certificate
Canada: UL 1950 – CSA 950 (complies with 73/23/EEC)
Europe/CE Mark: EN60950 (complies with 73/23/EEC)

Electromagnetic Compatibility (EMC)
Australia/New Zealand: AS/NZS 3548 (based on CISPR 22)
Canada: ICES-003, Class A
Europe, CE Mark: EN55022 (Class A); EN55024 and EN61000-3-2;-3-3 (complies with 89/336/EEC)
International: CISPR 22, Class A
Japan: VCCI, Class A
Korea: RRL, MIC 1997-41 & 1997-42
Russia: GOST 29216-91 & 50628-95
Taiwan: CNS13438, Class A
U.S.: FCC, Part 15, Class A

ORDERING INFORMATION

Network Sensor Software
DSNSS-E Dragon Network Sensor software for Ethernet
DSNSS-FE Dragon Network Sensor software for Fast Ethernet
DSNSS-GE Dragon Network Sensor software for Gigabit Ethernet

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

Dragon Policy Manager Software
DSEMS Dragon Enterprise Management software

Network Sensor Appliance
DSNSA-FE50-TX Dragon FE50 Network Sensor appliance for the small/branch office
DSNSA-FE200-TX Dragon FE200 Network Sensor Appliance for the regional office, small data center (Copper network interface card)
DSNSA-GE200-SX Dragon GE200 Network Sensor Appliance for the regional office, small data center (Fiber network interface card)
DSNSA-GE500-SX Dragon GE500 Network Sensor Appliance for the data center (Fiber network interface card)
DSNSA-GE500-TX Dragon GE500 Network Sensor Appliance for the data center (Copper Gigabit network interface card)

Dragon Management Appliances
DSEMA Dragon Enterprise Management Server
DSEPA Dragon Event Flow Processor

Sensor/Management Appliances
DSISA-TX INS2 Intergrated Network Sensor/Server (Copper network interface card)
DSISA-SX INS2 Integrated Network Sensor/Server (Fiber network interface card)
WARRANTY

As a customer-centric company, Enterasys is committed to providing the best possible workmanship and design in our product set. In the event that one of our products fails due to a defect in one of these factors, we have developed a comprehensive warranty that protects you and provides a simple way to get your products repaired as soon as possible.

SERVICE AND SUPPORT

Enterasys Networks understands that superior service and support is a critical component for your Business-Driven Network. The Enterasys SupportNet Portfolio—a suite of innovative and flexible service and support offerings—completes the Enterasys Business-Driven Network solution. SupportNet offers all the post-implementation support services you need—online, onsite or over the phone—to maintain 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 978-684-1000 or enterasys.com/corporate/contact/contact-sales.html

Enterasys Networks
Corporate Headquarters
50 Minuteman Road
Andover, MA 01810
USA